Identifikation und Beseitigung der Ausnutzung verschiedener Sicherheitslücken in Cisco TelePresence-Produkten

Identifikation und Beseitigung der Ausnutzung verschiedener Sicherheitslücken in Cisco TelePresence-Produkten

Beratungs-ID: cisco-amb-20110223-telepresence

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110223-telepresence

Version 1.1

Zur öffentlichen Veröffentlichung 2011 Februar 23 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zum PSIRT Cisco TelePresence-Paket mit Sicherheitsempfehlungen und bietet Identifizierungs- und Mitigationstechniken, die Administratoren auf Cisco Netzwerkgeräten bereitstellen können. Folgende individuelle Sicherheitsempfehlungen werden von dieser AMB abgedeckt:

- Mehrere Schwachstellen in Cisco TelePresence-Endgeräten
- Mehrere Schwachstellen in Cisco TelePresence Manager
- Mehrere Schwachstellen im Cisco TelePresence Multipoint Switch
- Mehrere Schwachstellen im Cisco TelePresence Recording Server

Merkmale der Schwachstelle

Cisco TelePresence-Produkte weisen mehrere Schwachstellen auf. In den folgenden Unterabschnitten werden die einzelnen PSIRT-Sicherheitsempfehlungen und die jeweiligen in den

einzelnen Hinweisen behandelten Schwachstellen zusammengefasst:

Cisco TelePresence-Endgeräte

Nicht authentifizierter CGI-Zugriff: Diese Schwachstelle kann ohne Authentifizierung und ohne Endbenutzerinteraktion per Fernzugriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor zur Ausnutzung wird über HTTP-Pakete mit TCP-Port 8082 bereitgestellt. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0372 zugewiesen.

CGI Command Injection: Diese Schwachstellen können per Remote-Zugriff mit Authentifizierung und ohne Benutzereingriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstellen kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor zur Ausnutzung besteht aus missgebildeten Secure Sockets Layer (SSL)-Paketen mit TCP-Port 443. Diesen Schwachstellen wurden die CVE-Identifikatoren CVE-2011-0373, CVE-2011-0374 und CVE-2011-0375 zugewiesen.

Offenlegung von TFTP-Informationen: Diese Schwachstelle kann remote ausgenutzt werden, ohne dass eine Authentifizierung erforderlich ist und die Endbenutzer nicht eingreifen müssen. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, können Informationen offen gelegt werden, sodass ein Angreifer Informationen über das betroffene Gerät erhalten kann. Der Angriffsvektor zur Ausnutzung wird über TFTP GET-Anforderungspakete mit UDP-Port 69 generiert. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0376 zugewiesen.

Malicious IP Address Injection: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann zu einer dauerhaften Denial of Service (DoS)-Bedingung führen. Der Angriffsvektor zur Ausnutzung besteht aus missgebildeten SOAP-Paketen (Simple Object Access Protocol), die die TCP-Ports 8081 und 9501 verwenden. Dieser Schwachstelle wurde die CVE-Kennung CVE-2011-0377 zugewiesen.

XML-RPC Command Injection: Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor zur Ausnutzung wird durch XML-RPC-Pakete mit den TCP-Ports 61441 und 61445 generiert. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0378 zugewiesen.

Cisco Discovery Protocol Remote Code Execution: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor für die Ausnutzung wird durch Cisco Discovery Protocol-Pakete generiert. Da das Cisco Discovery Protocol auf der Sicherungsschicht arbeitet, muss ein Angreifer einen Frame direkt an ein betroffenes Gerät senden können. Dieses Dokument enthält keine weiteren Informationen zu dieser Sicherheitslücke. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0379 zugewiesen.

Cisco TelePresence Manager

SOAP Authentication Bypass: Diese Schwachstelle kann ohne Authentifizierung und ohne Endbenutzerinteraktion per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, können die Berechtigungen erhöht werden. Der Angriffsvektor zur Ausnutzung besteht aus falsch geformten SOAP-Paketen mit den TCP-Ports 8080 und 8443. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0380 zugewiesen.

Java Remote Method Invocation (RMI) Command Injection: Diese Verwundbarkeit kann per Fernzugriff ausgenutzt werden, ohne dass eine Authentifizierung erforderlich ist und die Endbenutzer nicht eingreifen müssen. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor für die Ausnutzung besteht aus vorgefertigten Java RMI-Paketen, die die TCP-Ports 1100 und 32000 verwenden. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0381 zugewiesen.

Cisco Discovery Protocol Remote Code Execution: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung beliebigen Codes ermöglichen. Der Angriffsvektor für die Ausnutzung besteht aus Cisco Discovery Protocol-Paketen. Da das Cisco Discovery Protocol auf der Sicherungsschicht arbeitet, muss ein Angreifer einen Frame direkt an ein betroffenes Gerät senden können. Dieses Dokument enthält keine weiteren Informationen zu dieser Sicherheitslücke. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0379 zugewiesen.

Cisco TelePresence Multipoint Switch

Nicht authentifizierter Java Servlet Access: Diese Schwachstellen können ohne Authentifizierung und ohne Eingreifen der Endbenutzer per Fernzugriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstellen kann die Privilegien erhöhen. Der Angriffsvektor zur Ausnutzung besteht aus HTTP-Paketen, die mit TCP-Ports 80 und 8080 erstellt wurden, und SSL-Paketen, die mit TCP-Port 443 erstellt wurden. Diesen Schwachstellen wurden die CVE-Identifikatoren CVE-2011-0383 und CVE-2011-0384 zugewiesen.

Nicht authentifizierter Upload beliebiger Dateien: Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers per Fernzugriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor zur Ausnutzung besteht aus HTTP-Paketen, die TCP-Port 80 und SSL-Pakete, die TCP-Port 443 verwenden. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0385 zugewiesen.

Cisco Discovery Protocol Remote Code Execution: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung beliebigen Codes ermöglichen. Der Angriffsvektor für die Ausnutzung besteht aus Cisco Discovery Protocol-Paketen. Da das Cisco Discovery Protocol auf der Sicherungsschicht arbeitet, muss ein Angreifer einen Frame direkt an ein betroffenes Gerät senden können. Dieses Dokument enthält keine weiteren Informationen zu dieser Sicherheitslücke. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0379 zugewiesen.

Unauthorized Servlet Access: Diese Schwachstelle kann per Remote-Zugriff mit Authentifizierung und ohne Benutzereingriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Privilegien erhöhen. Der Angriffsvektor für die Ausnutzung besteht aus HTTP-Paketen mit TCP-Port 80 und SSL-Paketen mit TCP-Port 443. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0387 zugewiesen.

Java RMI Denial of Service: Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung besteht aus erstellten Java RMI-Paketen mit TCP-Port 8999. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0388

zugewiesen.

Real-Time Transport Control Protocol (RTCP) Denial of Service: Diese Schwachstelle kann ohne Authentifizierung und ohne Endbenutzerinteraktion per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung besteht in schädlichen UDP-Paketen, die an einen überwachenden RTCP-Steuerungsport gesendet werden, der zufällig ausgewählt und während der Einrichtung der Gesprächsverbindung ausgehandelt wird. Ein Angreifer könnte diese Verwundbarkeit mit gefälschten Paketen ausnutzen. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0389 zugewiesen.

XML-RPC Denial of Service: Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers remote ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor für die Ausnutzung besteht aus XML-RPC-Paketen, die den TCP-Port 9000 verwenden. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0390 zugewiesen.

Cisco TelePresence Recording Server

Nicht authentifizierter Java Servlet Access: Diese Schwachstelle kann ohne Authentifizierung und ohne Endbenutzerinteraktion remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Privilegien erhöhen. Der Angriffsvektor zur Ausnutzung besteht aus HTTP-Paketen, die mit TCP-Ports 80 und 8080 erstellt wurden, und SSL-Paketen, die mit TCP-Port 443 erstellt wurden. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0383 zugewiesen.

CGI Command Injection: Diese Verwundbarkeit kann ohne Authentifizierung und ohne Endbenutzer-Interaktion per Fernzugriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor für die Ausnutzung wird über SSL-Pakete mit TCP-Port 443 bereitgestellt. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0382 zugewiesen.

Nicht authentifizierter Upload beliebiger Dateien: Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers per Fernzugriff ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der Angriffsvektor zur Ausnutzung besteht aus HTTP-Paketen, die TCP-Port 80 und SSL-Pakete, die TCP-Port 443 verwenden. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0385 zugewiesen.

XML-RPC Arbitrary File Overwrite (Überschreiben beliebiger XML-RPC-Dateien): Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers per Remote-Zugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung besteht aus falsch geformten XML-RPC-Paketen mit den TCP-Ports 12102 und 12104. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0386 zugewiesen.

Cisco Discovery Protocol Remote Code Execution: Diese Schwachstelle kann ohne Authentifizierung und ohne Benutzereingriff remote ausgenutzt werden. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann die Ausführung von beliebigem Code ermöglichen. Der

Angriffsvektor für die Ausnutzung wird durch Cisco Discovery Protocol-Pakete generiert. Da das Cisco Discovery Protocol auf der Sicherungsschicht arbeitet, muss ein Angreifer einen Frame direkt an ein betroffenes Gerät senden können. Dieses Dokument enthält keine weiteren Informationen zu dieser Sicherheitslücke. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0379 zugewiesen.

Ad-Hoc Recording Denial of Service: Diese Schwachstelle kann ohne Authentifizierung und ohne Endbenutzer-Interaktion per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung wird über HTTP-Pakete mit TCP-Port 80 generiert. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0391 zugewiesen.

Java RMI Denial of Service: Diese Schwachstelle kann ohne Authentifizierung und ohne Eingreifen des Endbenutzers per Fernzugriff ausgenutzt werden. Wenn diese Schwachstelle erfolgreich ausgenutzt wird, kann dies zu einer Diensteverweigerung (Denial of Service, DoS) führen. Wiederholte Versuche, diese Schwachstelle auszunutzen, können zu einem anhaltenden DoS-Zustand führen. Der Angriffsvektor zur Ausnutzung besteht aus erstellten Java RMI-Paketen mit TCP-Port 8999. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0388 zugewiesen.

Nicht authentifizierte XML-RPC-Schnittstelle: Diese Schwachstelle kann lokal ausgenutzt werden, ohne dass eine Authentifizierung erforderlich ist und die Endbenutzer nicht eingreifen müssen. Eine erfolgreiche Ausnutzung dieser Verwundbarkeit kann zur Ausführung willkürlicher Aktionen führen. Der Angriffsvektor für die Ausnutzung besteht aus XML-RPC-Paketen, die den TCP-Port 8080 verwenden. Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-0392 zugewiesen.

Informationen zu anfälliger, nicht betroffener und fester Software finden Sie in den einzelnen PSIRT-Sicherheitsempfehlungen unter den folgenden Links:

- Mehrere Schwachstellen in Cisco TelePresence-Endgeräten
- Mehrere Schwachstellen in Cisco TelePresence Manager
- Mehrere Schwachstellen im Cisco TelePresence Multipoint Switch
- Mehrere Schwachstellen im Cisco TelePresence Recording Server

Überblick über die Risikominderungstechnik

Cisco Geräte bieten eine Reihe von Gegenmaßnahmen für diese Sicherheitslücken. Den Administratoren wird empfohlen, diese Schutzmethoden als allgemeine Best Practices für die Sicherheit von Infrastrukturgeräten und des Datenverkehrs im Netzwerk zu betrachten. Dieser Abschnitt des Dokuments bietet einen Überblick über diese Techniken.

Die Cisco IOS Software bietet mithilfe der folgenden Methoden einen effektiven Schutz vor Exploits:

- InfrastrukturZugriffskontrolllisten (iACLs)
- Unicast Reverse Path Forwarding (Unicast-RPF)
- IP Source Guard (IPSG)

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, diese Schwachstellen auszunutzen, und überprüfen die Quell-IP-Adresse dieser Pakete.

Die ordnungsgemäße Bereitstellung und Konfiguration von Unicast RPF bietet einen effektiven Schutz vor Angriffen, bei denen Pakete mit gefälschten Quell-IP-Adressen verwendet werden. Unicast-RPF sollte so nahe wie möglich an allen Datenverkehrsquellen bereitgestellt werden.

Die ordnungsgemäße Bereitstellung und Konfiguration von IPSG bietet einen effektiven Schutz vor Spoofing-Angriffen auf der Zugriffsebene.

Die Cisco Adaptive Security Appliance der Serie ASA 5500 und das Cisco Firewall Services Module (FWSM) für Cisco Catalyst-Switches der Serie 6500 und Cisco Router der Serie 7600 bieten folgende effektive Möglichkeiten zur Vermeidung von Exploits:

- Transit-Zugriffskontrolllisten (tACLs)
- Unicast RPF

Diese Schutzmechanismen filtern und löschen Pakete, die versuchen, diese Schwachstellen auszunutzen, und überprüfen die Quell-IP-Adresse dieser Pakete.

Die effektive Nutzung von Cisco Intrusion Prevention System (IPS)-Ereignisaktionen bietet Transparenz und Schutz vor Angriffen, die diese Schwachstellen ausnutzen.

Cisco IOS NetFlow-Datensätze bieten Transparenz für netzwerkbasierte Exploit-Versuche.

Die Firewalls Cisco IOS Software, Cisco ASA und FWSM bieten Transparenz durch Syslog-Meldungen und Zählerwerte, die in der Ausgabe der **show-**Befehle angezeigt werden.

Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance bietet ebenfalls Transparenz für Vorfälle, Abfragen und Ereignisberichte.

Weitere Informationen zu den verschiedenen Aspekten, die bei der Sicherung einer Cisco TelePresence-Umgebung berücksichtigt werden müssen, finden Sie im Cisco TelePresence Hardening Guide.

Risikomanagement

Den Unternehmen wird empfohlen, die potenziellen Auswirkungen dieser Schwachstellen anhand ihrer Standardprozesse zur Risikobewertung und -minderung zu ermitteln. Triage bezieht sich auf das Sortieren von Projekten und die Priorisierung von Bemühungen, die am wahrscheinlichsten erfolgreich sein werden. Cisco hat Dokumente bereitgestellt, die Unternehmen bei der Entwicklung einer risikobasierten Triage-Funktion für ihre Informationssicherheitsteams unterstützen. Risikoanalyse für Ankündigungen zu Sicherheitslücken sowie Risikoanalyse und -prototyping unterstützen Unternehmen bei der Entwicklung wiederholbarer Sicherheitsevaluierungs- und Reaktionsprozesse.

Gerätespezifische Eindämmung und Identifizierung

Vorsicht: Die Effektivität jeglicher Eindämmungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischem Auftrag ab. Prüfen Sie wie bei jeder Konfigurationsänderung die Auswirkungen dieser Konfiguration, bevor Sie die Änderung übernehmen.

Spezifische Informationen zur Risikominderung und Identifizierung sind für diese Geräte verfügbar:

- Cisco IOS-Router und -Switches
- Cisco IOS-NetFlow
- Cisco ASA und FWSM-Firewalls
- Cisco Intrusion Prevention System
- Cisco Security Monitoring, Analysis and Response System

Cisco IOS-Router und -Switches

Eindämmung: Infrastruktur-Zugriffskontrolllisten

Um Infrastrukturgeräte zu schützen und das Risiko, die Auswirkungen und die Effektivität direkter Angriffe auf die Infrastruktur zu minimieren, sollten Administratoren Infrastruktur-Zugriffskontrolllisten (iACLs) implementieren, um die Durchsetzung von Richtlinien für den an Infrastrukturgeräte gesendeten Datenverkehr zu ermöglichen. Administratoren können eine iACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen an die Geräte der Infrastruktur gesendet wird. Um einen maximalen Schutz für Infrastrukturgeräte zu gewährleisten, sollten bereitgestellte iACLs in Eingangsrichtung auf alle Schnittstellen angewendet werden, für die eine IP-Adresse konfiguriert wurde. Eine iACL-Problemumgehung kann keinen vollständigen Schutz vor diesen Schwachstellen bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die iACL-Richtlinie verweigert nicht autorisierte Pakete mit den folgenden Protokollen/Ports, die an betroffene Geräte gesendet werden:

- TCP-Port 80
- TCP-Port 443
- TCP-Port 1100
- TCP-Port 8080
- TCP-Port 8081
- TCP-Port 8082
- TCP-Port 8443
- TCP-Port 8999
- TCP-Port 9000
- TCP-Port 9501
- TCP-Port 12102
- TCP-Port 12104
- TCP-Port 32000
- TCP-Port 61441
- TCP-Port 61445
- UDP-Port 69

Im folgenden Beispiel ist 192.168.60.0/24 der IP-Adressraum, der von den betroffenen Geräten verwendet wird. Der Host unter 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird. Wenn möglich, sollte sich der Infrastruktur-Adressraum vom Adressraum unterscheiden, der für Benutzer- und Service-Segmente verwendet wird. Mit dieser Adressierungsmethode können Sie iACLs erstellen und bereitstellen.

Weitere Informationen zu iACLs finden Sie unter Protecting Your Core: Infrastructure Protection Access Control Lists (Schützen Ihres Kerns: Zugriffskontrolllisten für Infrastrukturschutz).

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 80
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 1100 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8080 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 8081 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8999 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 9000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 12102 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 12104 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 32000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445 permit udp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 69 ! !-- The following vulnerability-specific access
control entries !-- (ACEs) can aid in identification of attacks ! deny tcp any
192.168.60.0 0.0.0.255 eq 80 deny tcp any 192.168.60.0 0.0.0.255 eq 443 deny tcp any
192.168.60.0 0.0.0.255 eq 1100 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 deny tcp
any 192.168.60.0 0.0.0.255 eq 8081 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 deny
tcp any 192.168.60.0 0.0.0.255 eq 8443 deny tcp any 192.168.60.0 0.0.0.255 eq 8999
deny tcp any 192.168.60.0 0.0.0.255 eq 9000 deny tcp any 192.168.60.0 0.0.0.255 eq
9501 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 deny tcp any 192.168.60.0 0.0.0.255
eq 12104 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 deny tcp any 192.168.60.0
0.0.0.255 eq 61441 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 deny udp any
192.168.60.0 0.0.0.255 eq 69 ! !-- Explicit deny ACE for traffic sent to addresses
configured within !-- the infrastructure address space ! deny ip any 192.168.60.0
0.0.0.255 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-
- with existing security policies and configurations ! !-- Apply iACL to interfaces
in the ingress direction ! interface GigabitEthernet0/0 ip access-group
Infrastructure-ACL-Policy in
```

Beachten Sie, dass das Filtern mit einer Schnittstellenzugriffsliste die Übertragung von nicht erreichbaren ICMP-Nachrichten zurück an die Quelle des gefilterten Datenverkehrs auslöst. Das Generieren dieser Nachrichten könnte den unerwünschten Effekt einer erhöhten CPU-Auslastung auf dem Gerät haben. In Cisco IOS-Software ist nicht-erreichbare Generation ICMP auf ein Paket alle 500 Millisekunden standardmäßig begrenzt. Die Erzeugung von nicht erreichbaren ICMP-Nachrichten kann mit dem Schnittstellenkonfigurationsbefehl no ip unreachables deaktiviert werden. Die Durchsatzbegrenzung "ICMP unreachable" kann mithilfe des globalen Konfigurationsbefehls ip icmp rate-limit unreachable interval-in-ms vom Standard abgesetzt werden.

Eindämmung: Spoofing-Schutz

Unicast Reverse Path Forwarding

Eine der in diesem Dokument beschriebenen Schwachstellen kann durch gefälschte IP-Pakete ausgenutzt werden. Administratoren können Unicast Reverse Path Forwarding (Unicast RPF) als Schutzmechanismus gegen Spoofing bereitstellen und konfigurieren.

Unicast-RPF wird auf Schnittstellenebene konfiguriert und kann Pakete erkennen und verwerfen, denen eine verifizierbare Quell-IP-Adresse fehlt. Administratoren sollten sich nicht darauf verlassen, dass Unicast RPF einen vollständigen Spoofing-Schutz bietet, da gefälschte Pakete über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen können, wenn eine geeignete Rückgaberoute zur Quell-IP-Adresse vorhanden ist. Den Administratoren wird

empfohlen, während der Bereitstellung dieser Funktion sicherzustellen, dass der entsprechende Unicast-RPF-Modus (flexibel oder strikt) konfiguriert wird, da legitimer Datenverkehr, der das Netzwerk durchquert, verworfen werden kann. In einer Unternehmensumgebung kann Unicast-RPF am Internet-Edge und auf der internen Zugriffsebene der benutzerunterstützenden Layer-3-Schnittstellen aktiviert werden.

Weitere Informationen finden Sie im Funktionsleitfaden zur Unicast Reverse Path Forwarding Loose Mode.

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie im Whitepaper Understanding Unicast Reverse Path Forwarding Applied Intelligence.

IP-Quellschutz

IP Source Guard (IPSG) ist eine Sicherheitsfunktion, die den IP-Datenverkehr an nicht gerouteten Layer-2-Schnittstellen beschränkt, indem Pakete auf Basis der DHCP-Snooping-Bindungsdatenbank und manuell konfigurierter IP-Source-Bindings gefiltert werden. Administratoren können IPSG verwenden, um Angriffe eines Angreifers zu verhindern, der versucht, Pakete durch Fälschung der Quell-IP-Adresse und/oder der MAC-Adresse zu fälschen. Bei ordnungsgemäßer Bereitstellung und Konfiguration bietet IPSG in Verbindung mit dem Unicast RPF im strikten Modus den effektivsten Spoofing-Schutz für die in diesem Dokument beschriebenen Schwachstellen.

Weitere Informationen zur Bereitstellung und Konfiguration von IPSG finden Sie unter Konfigurieren der DHCP-Funktionen und von IP Source Guard.

Identifikation: Infrastruktur-Zugriffskontrolllisten

Nachdem der Administrator die iACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl show ip access-lists die Pakete der folgenden Protokolle/Ports, die auf Schnittstellen gefiltert wurden, auf die die iACL angewendet wird:

- TCP-Port 80
- TCP-Port 443
- TCP-Port 1100
- TCP-Port 8080
- TCP-Port 8081
- TCP-Port 8082
- TCP-Port 8443
- TCP-Port 8999
- TCP-Port 9000
- TCP-Port 9501
- TCP-Port 12102
- TCP-Port 12104
- TCP-Port 32000
- TCP-Port 61441
- TCP-Port 61445
- UDP-Port 69

Administratoren sollten gefilterte Pakete untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für show ip access-lists:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq www
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1100
    40 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8081
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082
    70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 (1 match)
    80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8999
    90 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9000
    100 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501
    110 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12102
    120 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12104
    130 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 32000
    140 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441
    150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445
    160 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq tftp
    170 deny tcp any 192.168.60.0 0.0.0.255 eq www (703 matches)
    180 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (213 matches)
    190 deny tcp any 192.168.60.0 0.0.0.255 eq 1100 (95 matches)
    200 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (115 matches)
    210 deny tcp any 192.168.60.0 0.0.0.255 eq 8081 (119 matches)
    220 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 (86 matches)
    230 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (125 matches)
    240 deny tcp any 192.168.60.0 0.0.0.255 eq 8999 (63 matches)
    250 deny tcp any 192.168.60.0 0.0.0.255 eq 9000 (3 matches)
    260 deny tcp any 192.168.60.0 0.0.0.255 eq 9501 (142 matches)
    270 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 (127 matches)
    280 deny tcp any 192.168.60.0 0.0.0.255 eq 12104 (132 matches)
    290 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 (125 matches)
    300 deny tcp any 192.168.60.0 0.0.0.255 eq 61441 (110 matches)
    310 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 (114 matches)
    320 deny udp any 192.168.60.0 0.0.0.255 eq tftp (218 matches)
    330 deny ip any 192.168.60.0 0.0.0.255 (9 matches)
router#
```

Im vorherigen Beispiel hat access list Infrastructure-ACL-Policy die folgenden Pakete verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden:

- 703 HTTP-Pakete an TCP-Port 80 (www) für ACE-Leitung 170
- 213 SSL-Pakete auf TCP-Port 443 für ACE-Leitung 180
- 95 Pakete an TCP-Port 1100 für ACE-Leitung 190
- 115 Pakete an TCP-Port 8080 für ACE-Leitung 200
- 119 Pakete an TCP-Port 8081 für ACE-Leitung 210
- 86 Pakete an TCP-Port 8082 für ACE-Leitung 220
- 125 Pakete an TCP-Port 8443 für ACE-Leitung 230
- 63 Pakete auf TCP-Port 8999 für ACE-Leitung 240
- 3 Pakete auf TCP-Port 9000 für ACE-Leitung 250
- 142 Pakete auf TCP-Port 9501 für ACE-Leitung 260
- 127 Pakete an TCP-Port 12102 für ACE-Leitung 270
- 132 Pakete an TCP-Port 12104 für ACE-Leitung 280
- 125 Pakete an TCP-Port 32000 für ACE-Leitung 290
- 110 Pakete an TCP-Port 61441 für ACE-Leitung 300
- 114 Pakete an TCP-Port 61445 für ACE-Leitung 310
- 218 TFTP-Pakete auf UDP-Port 69 für ACE-Leitung 320

Weitere Informationen zur Untersuchung von Vorfällen mithilfe von ACE-Zählern und Syslog-Ereignissen finden Sie im Whitepaper Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence.

Administratoren können den Embedded Event Manager verwenden, um eine Instrumentierung bereitzustellen, wenn bestimmte Bedingungen erfüllt sind, z. B. ACE-Zählerzugriffe. Das Whitepaper Embedded Event Manager in a Security Context von Applied Intelligence enthält weitere Informationen zur Verwendung dieser Funktion.

Identifizierung: Protokollierung der Zugriffsliste

Die Option log and log-input access control list (ACL) bewirkt, dass Pakete protokolliert werden, die zu bestimmten ACEs passen. Die Option log-input ermöglicht die Protokollierung der Eingangsschnittstelle zusätzlich zu den IP-Adressen und -Ports für die Paketquelle und das Ziel.

Achtung: Die Protokollierung von Zugriffskontrolllisten kann sehr CPU-intensiv sein und muss mit äußerster Vorsicht verwendet werden. Faktoren, die die Auswirkungen der ACL-Protokollierung auf die CPU verstärken, sind die Protokollgenerierung, die Protokollübertragung und das Prozess-Switching für die Weiterleitung von Paketen, die mit protokollfähigen ACEs übereinstimmen.

Für Cisco IOS-Software kann der Befehl "ip access-list logging interval-in-ms" die Auswirkungen des durch die ACL-Protokollierung induzierten Prozesswechsels begrenzen. Der Befehl logging rate-limit rate-per-second [except loglevel] begrenzt die Auswirkungen der Protokollgenerierung und -übertragung.

Die CPU-Auswirkungen der ACL-Protokollierung können mithilfe optimierter ACL-Protokollierung in der Hardware auf den Cisco Catalyst Switches der Serie 6500 und den Cisco Routern der Serie 7600 mit der Supervisor Engine 720 oder der Supervisor Engine 32 berücksichtigt werden.

Weitere Informationen zur Konfiguration und Verwendung der ACL-Protokollierung finden Sie im Whitepaper Understanding Access Control List Logging Applied Intelligence.

Identifizierung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Wenn Unicast RPF ordnungsgemäß in der gesamten Netzwerkinfrastruktur bereitgestellt und konfiguriert ist, können Administratoren den internen Steckplatz/Port des Schnittstellentyps "show cef", die **show ip interface,** die **show cef drop-Funktion**, die **Funktion "show ip cef switching statistics"** und die **show ip traffic-**Befehle verwenden, **um die Anzahl der von Unicast RPF blockierten Pakete zu identifizieren.**

Hinweis: Ab Version 12.4(20)T der Cisco IOS-Software wurde der Befehl **show ip cef switching** durch die **Funktion show ip cef switching statistics** ersetzt.

Hinweis: Der Befehl **show | Begin** regex and **show** command **| include** regex-Befehlsmodifizierer werden in den folgenden Beispielen verwendet, um die Ausgabe zu minimieren, die Administratoren analysieren müssen, um die gewünschten Informationen anzuzeigen. Weitere Informationen zu Befehlsmodifizierern finden Sie in den Abschnitten show command in der Cisco IOS Configuration Fundamentals Command Reference.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop

ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

Hinweis: show cef interface type slot/port **internal** ist ein ausgeblendeter Befehl, der vollständig in die Kommandozeile eingegeben werden muss. Die Befehlsvervollständigung steht dafür nicht zur Verfügung.

```
router#show ip interface GigabitEthernet 0/0 | begin verify

        IP verify source reachable-via RX, allow default, allow self-ping
        18 verification drops
        0 suppressed verification drops
router#
```

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj  ChkSum_Err
RP            27           0           0          18            0           0
router#
```

```
router#show ip cef switching statistics feature
IPv4 CEF input features:
Path   Feature                Drop    Consume       Punt  Punt2Host Gave route
RP PAS uRPF                     18          0          0          0          0
Total                           18          0          0          0          0
--      CLI Output Truncated       --
router#
```

```
router#show ip traffic | include RPF
           18 no route, 18 unicast RPF, 0 forced drop
router#
```

Im vorhergehenden Abschnitt **show cef drop**, **show ip cef switching statistics feature** and **show ip traffic** example, Unicast RPF hat **18** global **empfangene IP-Pakete** an allen Schnittstellen mit konfiguriertem Unicast RPF verworfen, weil die Quelladresse der IP-Pakete in der Forwarding Information Base von Cisco Express Forwarding nicht verifiziert werden konnte.

Cisco IOS-NetFlow

Identifizierung: Identifikation des Datenverkehrsflusses mithilfe von NetFlow-Datensätzen

Administratoren können Cisco IOS NetFlow auf Cisco IOS-Routern und -Switches konfigurieren, um Datenverkehrsflüsse zu identifizieren, die diese Schwachstellen ausnutzen können. Den Administratoren wird empfohlen, Datenflüsse zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen, oder ob es sich um legitime Datenflüsse handelt.

```
router#show ip cache flow

IP packet size distribution (1779 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .323 .676 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  183 active, 3913 inactive, 364 added
```

```
  4883 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW             16      0.0         7    40      0.0       0.0      15.7
TCP-other          126      0.0         3    40      0.1       0.0      15.4
UDP-TFTP             7      0.0         6    28      0.0       0.0      15.6
UDP-other           32      0.0         6    28      0.0       0.0      15.4
Total:             181      0.0         4    36      0.1       0.0      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.21.36   Et0/1         192.168.60.17   11 CD3E 0045     1
Et0/0         192.168.100.31  Et0/1         192.168.60.210  06 8F8C 044C     6
Et0/0         192.168.100.14  Et0/1         192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1         192.168.60.19   06 C460 1F90     3
Et0/0         192.168.100.235 Et0/1         192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.159.166 Et0/1         192.168.90.53   11 62E2 B413    10
Et0/0         192.168.100.164 Et0/1         192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1         192.168.60.30   06 E440 1F92     6
Et0/0         192.168.12.204  Et0/1         192.168.162.10  11 39D3 9273    10
Et0/0         192.168.100.211 Et0/1         192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1         192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1         192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2327     4
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2328     4
Et0/0         192.168.194.210 Et0/1         192.168.4.64    11 85DE BE0C     5
Et0/0         192.168.100.171 Et0/1         192.168.60.215  06 84F3 1F91     1
Et0/0         192.168.100.121 Et0/1         192.168.60.165  06 15A0 2F48     8
Et0/0         192.168.100.97  Et0/1         192.168.60.22   06 0951 2327     1
Et0/0         192.168.100.221 Et0/1         192.168.60.170  06 DBCF 0050    10
Et0/0         192.168.6.90    Et0/1         192.168.243.120 06 14E7 773D    10
Et0/0         192.168.100.174 Et0/1         192.168.60.239  06 0414 1F91     5
Et0/0         192.168.100.51  Et0/1         192.168.60.109  06 EF9D 251D     2
Et0/0         192.168.78.53   Et0/1         192.168.60.37   11 07A2 0045     2
Et0/0         192.168.164.19  Et0/1         192.168.201.180 06 FA1C 557B     5
Et0/0         192.168.66.15   Et0/1         192.168.155.182 11 FBC6 585A     3
Et0/0         192.168.100.208 Et0/1         192.168.60.137  06 BEC3 20FB     1
Et0/0         192.168.100.43  Et0/1         192.168.60.70   06 5E31 01BB    14
Et0/0         192.168.100.43  Et0/1         192.168.60.0    06 0FAA F001     1
Et0/0         192.168.29.205  Et0/1         192.168.240.249 11 71B3 8F9C     8
Et0/0         192.168.100.179 Et0/1         192.168.60.214  06 A2C4 F005     4
Et0/0         192.168.89.13   Et0/1         192.168.204.26  11 1D17 2CB0    11
router#
```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für:

- HTTP an TCP-Port 80 (Hexadezimalwert 0050)
- SSL auf TCP-Port 443 (Hexadezimalwert 01BB)
- TCP-Port 1100 (Hexadezimalwert 044C)
- TCP-Port 8080 (Hexadezimalwert 1F90)
- TCP-Port 8081 (Hexadezimalwert 1F91)
- TCP-Port 8082 (Hexadezimalwert 1F92)
- TCP-Port 8443 (Hex-Wert 20 FB)
- TCP-Port 8999 (Hexadezimalwert 2327)

- TCP-Port 9000 (Hexadezimalwert 2328)
- TCP-Port 9501 (Hexadezimalwert 251D)
- TCP-Port 12102 (Hexadezimalwert 2F46)
- TCP-Port 12104 (Hexadezimalwert 2F48)
- TCP-Port 32000 (Hexadezimalwert 7D00)
- TCP-Port 61441 (Hexadezimalwert F001)
- TCP-Port 61445 (Hexadezimalwert F005)
- TFTP auf UDP-Port 69 (Hexadezimalwert 0045)

Dieser Datenverkehr wird an Adressen im Adressblock 192.168.60.0/24 gesendet, der für Infrastrukturgeräte verwendet wird. Die Pakete in diesen Flows können gefälscht sein und einen Versuch anzeigen, diese Schwachstellen auszunutzen. Den Administratoren wird empfohlen, diese Datenflüsse mit der Basisauslastung für Datenverkehr zu vergleichen, der über die oben genannten Protokolle/Ports gesendet wird. Außerdem sollten sie die Flüsse untersuchen, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts oder Netzwerken stammen. Um nur die Datenverkehrsflüsse für Pakete auf den oben genannten Ports/Protokollen anzuzeigen, muss der Befehl show ip cache flow | include SrcIf|__11_.*0045 zeigt die zugehörigen UDP NetFlow-Datensätze wie folgt an:

UDP-Datenflüsse

```
router#show ip cache flow | include SrcIf|_11_.*0045
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

Et0/0         192.168.54.222  Et0/1         192.168.60.43   11 7947 0045     3
Et0/0         192.168.247.117 Et0/1         192.168.60.169  11 45FB 0045     1
Et0/0         192.168.250.16  Et0/1         192.168.60.79   11 66AC 0045    10
Et0/0         192.168.121.112 Et0/1         192.168.60.36   11 6725 0045    16
Et0/0         192.168.243.192 Et0/1         192.168.60.225  11 2B52 0045     1
router#
```

Um nur die Datenverkehrsflüsse für Pakete auf den oben genannten Ports/Protokollen anzuzeigen, muss der Befehl show ip cache flow | include SrcIf|__06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F005)_ zeigt die zugehörigen TCP NetFlow-Datensätze wie folgt an:

TCP-Flows

```
router#show ip cache flow | include
SrcIf|_06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F0
05)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.100.14  Et0/1         192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1         192.168.60.19   06 C460 1F90     3
Et0/0         192.168.100.235 Et0/1         192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.100.164 Et0/1         192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1         192.168.60.30   06 E440 1F92     6

Et0/0         192.168.100.211 Et0/1         192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1         192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1         192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2327     4
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2328     4

Et0/0         192.168.100.121 Et0/1         192.168.60.165  06 15A0 2F48     8
```

```
Et0/0          192.168.100.208 Et0/1          192.168.60.137   06 BEC3 20FB     1
Et0/0          192.168.100.43  Et0/1          192.168.60.70    06 5E31 01BB    14
Et0/0          192.168.100.43  Et0/1          192.168.60.0     06 0FAA F001     1
Et0/0          192.168.100.179 Et0/1          192.168.60.214   06 A2C4 F005     4

Et0/0          192.168.100.209 Et0/1          192.168.60.19    06 C460 1F90     3
router#
```

Cisco ASA und FWSM-Firewalls

Eindämmung: Transit-Zugriffskontrolllisten

Um das Netzwerk vor Datenverkehr zu schützen, der am Eingangspunkt in das Netzwerk gelangt, z. B. Internetverbindungspunkte, Verbindungspunkte für Partner und Lieferanten oder VPN-Verbindungspunkte, sollten Administratoren tACLs bereitstellen, um die Richtlinien durchzusetzen. Administratoren können eine tACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr an den Eingangs-Access Points in das Netzwerk eindringt, oder indem sie autorisiertem Datenverkehr gestatten, das Netzwerk gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen zu passieren. Eine tACL-Problemumgehung kann keinen vollständigen Schutz vor diesen Schwachstellen bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die tACL-Richtlinie verweigert nicht autorisierte Pakete mit den folgenden Protokollen/Ports, die an betroffene Geräte gesendet werden:

- TCP-Port 80
- TCP-Port 443
- TCP-Port 1100
- TCP-Port 8080
- TCP-Port 8081
- TCP-Port 8082
- TCP-Port 8443
- TCP-Port 8999
- TCP-Port 9000
- TCP-Port 9501
- TCP-Port 12102
- TCP-Port 12104
- TCP-Port 32000
- TCP-Port 61441
- TCP-Port 61445
- UDP-Port 69

Im folgenden Beispiel ist 192.168.60.0/24 der IP-Adressraum, der von den betroffenen Geräten verwendet wird. Der Host unter 192.168.100.1 gilt als vertrauenswürdige Quelle, die Zugriff auf die betroffenen Geräte erfordert. Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird.

Weitere Informationen zu tACLs finden Sie in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 80 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 1100
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8080 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8081 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 8082 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 9000 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 12102 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 12104 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 61441 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 access-list tACL-Policy extended permit udp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 69 ! !-- The following vulnerability-
specific access control entries !-- (ACEs) can aid in identification of attacks !
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 80
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 1100
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8080
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8081
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8082
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9501
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12102
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12104
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61441
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61445
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 69 ! !--
Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing
security policies and configurations ! !-- Explicit deny for all other IP traffic !
access-list tACL-Policy extended deny ip any any ! !-- Apply tACL to interface(s) in
the ingress direction ! access-group tACL-Policy in interface outside
```

Eindämmung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Die in diesem Dokument beschriebenen Schwachstellen können durch gefälschte IP-Pakete ausgenutzt werden. Administratoren können Unicast RPF als Spoofing-Schutzmechanismus bereitstellen und konfigurieren.

Unicast-RPF wird auf Schnittstellenebene konfiguriert und kann Pakete erkennen und verwerfen, denen eine verifizierbare Quell-IP-Adresse fehlt. Administratoren sollten sich nicht darauf verlassen, dass Unicast RPF einen vollständigen Spoofing-Schutz bietet, da gefälschte Pakete über eine Unicast RPF-fähige Schnittstelle in das Netzwerk gelangen können, wenn eine geeignete Rückgaberoute zur Quell-IP-Adresse vorhanden ist. In einer Unternehmensumgebung kann Unicast-RPF am Internet-Edge und auf der internen Zugriffsebene der benutzerunterstützenden Layer-3-Schnittstellen aktiviert werden.

Weitere Informationen zur Konfiguration und Verwendung von Unicast RPF finden Sie in der Cisco

Security Appliance Command Reference for ip verify reverse path und im Whitepaper Understanding Unicast Reverse Path Forwarding Applied Intelligence.

Identifizierung: Transit-Zugriffskontrolllisten

Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl show access-list die folgenden gefilterten Protokolle/Ports identifizieren:

- TCP-Port 80
- TCP-Port 443
- TCP-Port 1100
- TCP-Port 8080
- TCP-Port 8081
- TCP-Port 8082
- TCP-Port 8443
- TCP-Port 8999
- TCP-Port 9000
- TCP-Port 9501
- TCP-Port 12102
- TCP-Port 12104
- TCP-Port 32000
- TCP-Port 61441
- TCP-Port 61445
- UDP-Port 69

Den Administratoren wird empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstellen auszunutzen. Beispielausgabe für show access-list tACL-Policy:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 31 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq www (hitcnt=55)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq https (hitcnt=765)
access-list tACL-Policy line 3 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=43)
access-list tACL-Policy line 4 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=265)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=18)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=77)
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=345)
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=137)
access-list tACL-Policy line 9 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=17)
access-list tACL-Policy line 10 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=36)
access-list tACL-Policy line 11 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=40)
access-list tACL-Policy line 12 extended permit tcp host 192.168.100.1
```

```
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=23)
access-list tACL-Policy line 13 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=109)
access-list tACL-Policy line 14 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=60)
access-list tACL-Policy line 15 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=95)
access-list tACL-Policy line 16 extended permit udp host 192.168.100.1
192.168.60.0 255.255.255.0 eq tftp (hitcnt=4567)
access-list tACL-Policy line 17 extended deny tcp any
192.168.60.0 255.255.255.0 eq www (hitcnt=28)
access-list tACL-Policy line 18 extended deny tcp any
192.168.60.0 255.255.255.0 eq https (hitcnt=169)
access-list tACL-Policy line 19 extended deny tcp any
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=93)
access-list tACL-Policy line 20 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=11)
access-list tACL-Policy line 21 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=9)
access-list tACL-Policy line 22 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=9)
access-list tACL-Policy line 23 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=34)
access-list tACL-Policy line 24 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=46)
access-list tACL-Policy line 25 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=6)
access-list tACL-Policy line 26 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=9)
access-list tACL-Policy line 27 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=11)
access-list tACL-Policy line 28 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=24)
access-list tACL-Policy line 29 extended deny tcp any
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=48)
access-list tACL-Policy line 30 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=32)
access-list tACL-Policy line 31 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=9)
access-list tACL-Policy line 32 extended deny udp any
192.168.60.0 255.255.255.0 eq tftp (hitcnt=78)
access-list tACL-Policy line 33 extended deny ip any any (hitcnt=4658)
firewall#
```

Im vorherigen Beispiel hat die Zugriffsliste tACL-Policy die folgenden Pakete verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden:

- 28 HTTP-Pakete an TCP-Port 80 (www) für ACE-Leitung 17
- 169 SSL-Pakete auf TCP-Port 443 (HTTPS) für ACE-Leitung 18
- 93 Pakete an TCP-Port 1100 für ACE-Leitung 19
- 11 Pakete an TCP-Port 8080 für ACE-Leitung 20
- 9 Pakete an TCP-Port 8081 für ACE-Leitung 21
- 9 Pakete an TCP-Port 8082 für ACE-Leitung 22
- 34 Pakete an TCP-Port 8443 für ACE-Leitung 23
- 46 Pakete an TCP-Port 8999 für ACE-Leitung 24
- 6 Pakete auf TCP-Port 9000 für ACE-Leitung 25
- 9 Pakete auf TCP-Port 9501 für ACE-Leitung 26
- 11 Pakete an TCP-Port 12102 für ACE-Leitung 27
- 24 Pakete an TCP-Port 12014 für ACE-Leitung 28

- 48 Pakete an TCP-Port 32000 für ACE-Leitung 29
- 32 Pakete an TCP-Port 61441 für ACE-Leitung 30
- 9 Pakete an TCP-Port 61445 für ACE-Leitung 31
- 78 TFTP-Pakete auf UDP-Port 69 (TFTP) für ACE-Leitung 32

Identifizierung: Firewall Access List, Syslog-Meldungen

Die Firewall-Syslog-Meldung 106023 wird für Pakete generiert, die von einem Zugriffskontrolleintrag (Access Control Entry, ACE) abgelehnt wurden, für die das Schlüsselwort log nicht vorhanden ist. Weitere Informationen zu dieser Syslog-Meldung finden Sie in Cisco ASA 5500 Series System Log Message, 8.2 - 106023.

Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 finden Sie unter Überwachung - Konfigurieren der Protokollierung. Informationen zur Konfiguration von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie im Monitoring the Firewall Services Module.

Im folgenden Beispiel zeigt die Protokollierung | grep regex extrahiert Syslog-Meldungen aus dem Protokollierungspuffer der Firewall. Diese Meldungen enthalten zusätzliche Informationen zu abgelehnten Paketen, die auf potenzielle Versuche hinweisen könnten, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Es ist möglich, verschiedene reguläre Ausdrücke mit dem grep-Schlüsselwort zu verwenden, um nach bestimmten Daten in den protokollierten Nachrichten zu suchen.

Weitere Informationen zur Syntax regulärer Ausdrücke finden Sie unter Erstellen eines regulären Ausdrucks.

```
firewall#show logging | grep 106023
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.215/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.173/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.225.47/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.156.169/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.191.223/1024
                  dst inside:192.168.60.103/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.177/8080 by access-group "tACL-Policy"
```

```
firewall#
```

Im vorherigen Beispiel zeigen die für die tACL-tACL-Richtlinie protokollierten Nachrichten HTTP-Pakete für TCP-Port 80, SSL-Pakete für TCP-Port 443, Pakete für TCP-Port 1100 und Pakete für TCP-Port 8080, die an den Adressblock gesendet werden, der den betroffenen Geräten zugewiesen ist.

Weitere Informationen zu Syslog-Meldungen für ASA Security Appliances finden Sie in Cisco ASA 5500 Series System Log Messages, 8.2. Weitere Informationen zu Syslog-Meldungen für FWSM finden Sie in den Protokollnachrichten des Catalyst Switches der Serie 6500 und des Cisco Routers der Serie 7600, Protokollierungssystem für Firewall-Services-Module.

Weitere Informationen zur Untersuchung von Vorfällen mithilfe von Syslog-Ereignissen finden Sie im Whitepaper Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence.

Identifizierung: Spoofing-Schutz mit Unicast Reverse Path Forwarding

Die Firewall-Syslog-Meldung 106021 wird für Pakete generiert, die von Unicast RPF abgelehnt wurden. Weitere Informationen zu dieser Syslog-Meldung finden Sie in Cisco ASA 5500 Series System Log Message, 8.2 - 106021.

Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 finden Sie unter Überwachung - Konfigurieren der Protokollierung. Informationen zur Konfiguration von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie im Monitoring the Firewall Services Module.

Im folgenden Beispiel **zeigt** die **Protokollierung | grep** regex extrahiert Syslog-Meldungen aus dem Protokollierungspuffer der Firewall. Diese Meldungen enthalten zusätzliche Informationen zu abgelehnten Paketen, die auf potenzielle Versuche hinweisen könnten, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Es ist möglich, verschiedene reguläre Ausdrücke mit dem **grep-**Schlüsselwort zu verwenden, um nach bestimmten Daten in den protokollierten Nachrichten zu suchen.

Weitere Informationen zur Syntax regulärer Ausdrücke finden Sie unter Erstellen eines regulären Ausdrucks.

```
firewall#show logging | grep 106021
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny TCP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
```

Der Befehl **show asp drop** kann außerdem die Anzahl der Pakete identifizieren, die von der Unicast RPF-Funktion verworfen wurden, wie im folgenden Beispiel gezeigt:

```
firewall#show asp drop frame rpf-violated
        Reverse-path verify failed                      11
firewall#
```

Im vorherigen Beispiel hat Unicast RPF **11 IP-Pakete** verworfen, die an Schnittstellen mit

konfiguriertem Unicast RPF empfangen wurden. Fehlende Ausgabe zeigt an, dass die Unicast-RPF-Funktion der Firewall keine Pakete verworfen hat.

Weitere Informationen zum Debuggen von Paketen oder Verbindungen, die über einen beschleunigten Sicherheitspfad verworfen wurden, finden Sie unter Cisco Security Appliance Command Reference (Cisco Security Appliance-Befehlsreferenz) für show asp drop.

Cisco Intrusion Prevention System

Eindämmung: Cisco IPS-Signaturereignisaktionen

Administratoren können die Appliances und Dienstmodule des Cisco Intrusion Prevention System (IPS) verwenden, um Bedrohungen zu erkennen und Versuche zu verhindern, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Diese Schwachstellen können durch die folgenden Signaturen erkannt werden:

- 32719-0: Cisco TelePresence Unauthentifizierte Remote-Ausführung beliebiger Befehle
- 33859-0: Cisco TelePresence-Endgerät CGI-Befehlseinspritzung
- 33860-0: Cisco TelePresence Multipoint Switch - Java Servlet Access
- 33860-1: Cisco TelePresence Multipoint Switch - Java Servlet Access
- 33861-0: Anfälligkeit von Cisco TelePresence Recording Server für die Befehlsausführung

32719-0: Cisco TelePresence Unauthentifizierte Remote-Ausführung beliebiger Befehle

Beginnend mit dem Signatur-Update S550 für Sensoren, auf denen Cisco IPS 6.x und höher ausgeführt wird, können diese Schwachstellen mit der Signatur 32719/0 erkannt werden (Signature Name: Cisco TelePresence UnAuthenticated Remote Arbitrary Command Execution). Signatur 32719/0 ist standardmäßig aktiviert, löst ein Ereignis mit hohem Schweregrad aus, weist eine Signaturtreue-Bewertung (SFR) von 90 auf und wird mit der Standardereignisaktion **product-alert** konfiguriert.

Signature 32719/0 wird ausgelöst, wenn versucht wird, eine nicht authentifizierte, entfernte, beliebige Befehlsausführungsschwachstelle in einem Cisco TelePresence-Endgerät auszunutzen, das über den TCP-Port 8082 gesendet wurde. Das Auslösen dieser Signatur kann auf einen möglichen Missbrauch dieser Sicherheitslücken hinweisen.

33859-0: Cisco TelePresence-Endgerät CGI-Befehlseinspritzung

Ab dem Signatur-Update S550 für Sensoren mit Cisco IPS 6.x und höher können diese Schwachstellen mit der Signatur 33859-0 erkannt werden (Signature Name: Cisco TelePresence Endpoint CGI Command Injection). Signatur 33859/0 ist standardmäßig aktiviert, löst ein Ereignis mit hohem Schweregrad aus, weist eine Signaturtreue-Bewertung (SFR) von 80 auf und wird mit der Standardereignisaktion **product-alert** konfiguriert.

Signature 33859/0 wird ausgelöst, wenn versucht wird, eine nicht authentifizierte, entfernte, beliebige Befehlsausführungsschwachstelle in einem Cisco TelePresence-Endgerät auszunutzen, das über den TCP-Port 8082 gesendet wurde. Das Auslösen dieser Signatur kann auf einen möglichen Missbrauch dieser Sicherheitslücken hinweisen.

33860-0: Cisco TelePresence Multipoint Switch - Java Servlet Access

Ab dem Signatur-Update S550 für Sensoren mit Cisco IPS 6.x und höher können diese Schwachstellen mit der Signatur 33860-0 erkannt werden (Signature Name: Cisco TelePresence Multipoint Switch Java Servlet Access). Signatur 33860/0 ist standardmäßig deaktiviert, löst ein Ereignis mit hohem Schweregrad aus, weist eine Signaturtreue-Bewertung (SFR) von 75 auf und wird mit der Standardereignisaktion **product-alert** konfiguriert.

Signatur 33860/0 wird ausgelöst, wenn der Zugriff mehrerer Java Servlets innerhalb des Cisco TelePresence Multipoint Switches erkannt wird, die über den TCP-Port 8080 gesendet werden. Das Auslösen dieser Signatur kann auf einen möglichen Missbrauch dieser Sicherheitslücken hinweisen.

Hinweis: Diese Signatur kann auf Geräten ohne Cisco TelePresence Multipoint Switches fehlerfrei ausgegeben werden. Weitere Untersuchungen sind erforderlich, um solche Vorrichtungen zu beseitigen.

33860-1: Cisco TelePresence Multipoint Switch - Java Servlet Access

Ab dem Signatur-Update S550 für Sensoren mit Cisco IPS 6.x und höher können diese Schwachstellen mit der Signatur 33860-1 erkannt werden (Signature Name: Cisco TelePresence Multipoint Switch Java Servlet Access). Signatur 33860/1 ist standardmäßig deaktiviert, löst ein Ereignis mit hohem Schweregrad aus, weist eine Signaturtreue-Bewertung (SFR) von 75 auf und wird mit der Standardereignisaktion **product-alert** konfiguriert.

Signatur 33860/1 wird ausgelöst, wenn der Zugriff mehrerer Java Servlets innerhalb des Cisco TelePresence Multipoint Switches erkannt wird, die über den TCP-Port 80 gesendet werden. Das Auslösen dieser Signatur kann auf einen möglichen Missbrauch dieser Sicherheitslücken hinweisen.

Hinweis: Diese Signatur kann auf Geräten ohne Cisco TelePresence Multipoint Switches fehlerfrei ausgegeben werden. Weitere Untersuchungen sind erforderlich, um solche Vorrichtungen zu beseitigen.

33861-0: Anfälligkeit von Cisco TelePresence Recording Server für die Befehlsausführung

Ab dem Signatur-Update S550 für Sensoren mit Cisco IPS 6.x und höher können diese Schwachstellen mit der Signatur 33861/0 erkannt werden (Signature Name: Cisco TelePresence Recording Server Command Execution Vulnerability). Signatur 33861/0 ist standardmäßig aktiviert, löst ein Ereignis mit hohem Schweregrad aus, weist eine Signaturtreue-Bewertung (SFR) von 90 auf und wird mit der Standardereignisaktion **product-alert** konfiguriert.

Diese Signatur wird ausgelöst, wenn ein Versuch erkannt wird, eine spezifische Schwachstelle bei der Befehlsausführung in Cisco TelePresence Recording Server auszunutzen. Diese Verwundbarkeit wird weiter dokumentiert in CVE-2011-0382.

Signatur 33861/0 ist eine Meta-Signatur und besteht aus mehreren Untersignaturen (Signature-IDs 33861-1 bis 33861-4), die alle ausgelöst werden müssen, damit die Meta-Signatur ausgelöst wird. Jede der einzelnen Untersignaturen hat daher keine Ereignisaktion für sich und gilt somit als Informations-Schweregrad-Ereignis.

Administratoren können Cisco IPS-Sensoren so konfigurieren, dass sie eine Ereignisaktion ausführen, wenn ein Angriff erkannt wird. Die konfigurierte Ereignisaktion führt eine präventive oder abschreckende Kontrolle durch, um den Schutz vor einem Angriff zu gewährleisten, der versucht, die in diesem Dokument beschriebenen Schwachstellen auszunutzen.

Cisco IPS-Sensoren sind am effektivsten, wenn sie im Inline-Schutzmodus in Verbindung mit einer Ereignisaktion bereitgestellt werden. Die automatische Prävention von Sicherheitsrisiken für Cisco IPS 6.x und höhere Sensoren, die im Inline-Schutzmodus bereitgestellt werden, bietet Schutz vor Bedrohungen bei einem Angriff, der versucht, die in diesem Dokument beschriebenen Schwachstellen auszunutzen. Der Schutz vor Bedrohungen wird durch eine Standardüberschreibung erreicht, die eine Ereignisaktion für ausgelöste Signaturen mit einem riskRatingValue von mehr als 90 ausführt.

Weitere Informationen zur Berechnung von Risikoeinstufung und Bedrohungseinstufung finden Sie unter Risikoeinstufung und Bedrohungseinstufung: Vereinfachtes IPS-Richtlinienmanagement.

Cisco Security Monitoring, Analysis and Response System

Identifikation: Cisco Security Monitoring, Analysis, and Response System Incidents

Die Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)-Appliance kann mithilfe der folgenden IPS-Signaturen Incidents in Bezug auf Ereignisse erzeugen, die mit den in diesem Dokument beschriebenen Schwachstellen zusammenhängen:

- 32719-0: Cisco TelePresence Unauthentifizierte Remote-Ausführung beliebiger Befehle
- 33859-0: Cisco TelePresence-Endgerät CGI-Befehlseinspritzung
- 33860-0: Cisco TelePresence Multipoint Switch - Java Servlet Access
- 33860-1: Cisco TelePresence Multipoint Switch - Java Servlet Access
- 33861-0: Anfälligkeit von Cisco TelePresence Recording Server für die Befehlsausführung

Nach dem Herunterladen des dynamischen Signatur-Updates für S550 wird mithilfe der folgenden Schlüsselwörter für die jeweiligen IPS-Signatur-IDs und des Abfragetyps **Alle übereinstimmenden Ereignis-Rohmeldungen** auf der Cisco Security MARS-Appliance ein Bericht bereitgestellt, in dem die durch die IPS-Signatur erstellten Vorfälle aufgelistet werden.

- **NR-32719/0** für IPS-Signatur 32719/0
- **NR-33859/0** für IPS-Signatur 33859/0
- **NR-33860/0** für IPS-Signatur 33860/0
- **NR-33860/1** für IPS-Signatur 33860/1
- **NR-33861** für IPS-Signaturen 33861/0 bis 33861/4

Ab der Version 4.3.1 und 5.3.1 der Cisco Security MARS-Appliances wird die Funktion zur Aktualisierung dynamischer Signaturen von Cisco IPS unterstützt. Diese Funktion lädt neue Signaturen von Cisco.com oder von einem lokalen Webserver herunter, verarbeitet und kategorisiert empfangene Ereignisse, die mit diesen Signaturen übereinstimmen, ordnungsgemäß und fügt sie in Prüfungsregeln und Berichte ein. Diese Updates ermöglichen die Ereignisnormalisierung und die Zuordnung von Ereignisgruppen. Außerdem können neue Signaturen von IPS-Geräten mithilfe der MARS-Appliance analysiert werden.

Achtung: Wenn keine dynamischen Signatur-Updates konfiguriert werden, werden Ereignisse, die diesen neuen Signaturen entsprechen, in Abfragen und Berichten als unbekannter Ereignistyp angezeigt. Da MARS diese Ereignisse nicht in die Überprüfungsregeln einbezieht, kann es vorkommen, dass keine Vorfälle für potenzielle Bedrohungen oder Angriffe innerhalb des Netzwerks erstellt werden.

Diese Funktion ist standardmäßig aktiviert, muss jedoch konfiguriert werden. Wenn sie nicht konfiguriert ist, wird die folgende Cisco Security MARS-Regel ausgelöst:

```
System Rule: CS-MARS IPS Signature Update Failure
```

Wenn diese Funktion aktiviert und konfiguriert ist, können Administratoren die aktuelle von MARS heruntergeladene Signaturversion ermitteln, indem sie "Hilfe" > "Info" auswählen und den IPS-Signaturversionswert überprüfen.

Zusätzliche Informationen zu dynamischen Signatur-Updates und Anweisungen zum Konfigurieren dynamischer Signatur-Updates sind für die Versionen Cisco Security MARS 4.3.1 und 5.3.1 verfügbar.

Zusätzliche Informationen

Dieses Dokument wird in der vorliegenden Form bereitgestellt und impliziert keine Garantie oder Gewährleistung, einschließlich der Gewährleistung der Marktgängigkeit oder Eignung für einen bestimmten Zweck. Die Nutzung der Informationen im Dokument oder den Materialien, die mit dem Dokument verknüpft sind, erfolgt auf Ihr eigenes Risiko. Cisco behält sich das Recht vor, dieses Dokument jederzeit zu ändern oder zu aktualisieren.

Revisionsverlauf

Version 1.1	25. Februar 2011	Aktualisiert, um Informationen zur Signatur-ID 33861-0 einzuschließen.
Version 1.0	23. Februar 2011	Erste Veröffentlichung.

Cisco Sicherheitsverfahren

Vollständige Informationen zur Meldung von Sicherheitslücken in Cisco Produkten, zum Erhalt von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Cisco Website unter https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dies beinhaltet Anweisungen für Presseanfragen bezüglich der Sicherheitshinweise von Cisco. Alle Cisco Sicherheitsankündigungen finden Sie unter http://www.cisco.com/go/psirt.

Zugehörige Informationen

- Cisco TelePresence - Leitfaden zur Absicherung
- Cisco Applied Mitigation Bulletins
- Cisco Security
- Cisco Security IntelliShield Alert Manager Service
- Cisco Leitfaden zum Absichern von Cisco IOS-Geräten
- Überblick über die XSS-Bedrohungsvektoren (Cross-Site Scripting)
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Cisco IOS NetFlow-Whitepaper

- NetFlow-Leistungsanalyse
- Cisco Network Foundation Protection - Whitepaper
- Cisco Network Foundation Protection - Präsentationen
- Erkennung von und Beseitigung von TTL-Ablaufangriffen
- Ein sicherheitsorientierter Ansatz für die IP-Adressierung
- Sichern der Tool Command Language auf Cisco IOS
- Cisco Firewall-Produkte - Startseite auf Cisco.com
- Cisco ACE Application Control Engine Module - Dokumentation
- Verbesserungen der Unicast Reverse Path Forwarding für den Internet Service Provider
- Cisco Intrusion Prevention System
- Cisco IPS-Signatur-Downloads
- Seite für die Suche nach Cisco IPS-Signaturen
- Cisco Security Monitoring, Analysis and Response System
- Common Vulnerabilities and Exposures (CVE)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.