Zusammenfassung der Cisco IOS- und IOS XE Software Security Advisory Bundled Publication, 23. März 2016

'+'Top of the section'+''); } function endA() { //alert("end"); document.write('

'); } function startExpandoIndentSubheader() { document.write('
'); } function endExpandoIndentSubheader() { document.write('
'); } function endIndent() { //alert("end"); document.write('

'+"+"+'[Expand all sections]'+' '+' [Collapse all sections]'+'+'+'Close Section'+'

Beratungs-ID: cisco-sa-20160323-Paket

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160323-bundle

Revision 1.0

Für die Veröffentlichung 2016, 23. März, 16:00 Uhr UTC (GMT)

Inhalt

Zusammenfassung
Softwareversionen und -korrekturen
Erwerb fester Software
Status dieser Mitteilung: Finale
Distribution
Revisionsverlauf
Cisco Sicherheitsverfahren

Zusammenfassung

Die Veröffentlichung der Cisco IOS und IOS XE Software Security Advisory Bundled Publication am 23. März 2016 umfasst sechs Cisco Security Advisories, die sechs Sicherheitslücken beschreiben. Eine vollständige Liste der Ratgeber und Links zu diesen finden Sie unter Cisco Event Response: Veröffentlichung der halbjährlichen Cisco IOS- und IOS XE Software Security Advisory.

Softwareversionen und -korrekturen

Bei Software-Upgrades sollten Kunden das Cisco Security Advisories and Responses-Archiv unter http://www.cisco.com/go/psirt konsultieren und nachfolgende Ratgeber konsultieren, um

herauszufinden, ob das Produkt verfügbar ist und eine komplette Upgrade-Lösung vorhanden ist.

In allen Fällen sollten Kunden sicherstellen, dass die Geräte, die aktualisiert werden sollen, über ausreichend Speicherplatz verfügen, und sicherstellen, dass die aktuelle Hardware- und Softwarekonfiguration weiterhin von der neuen Version ordnungsgemäß unterstützt wird. Wenn die Informationen nicht klar sind, sollten sich Kunden an das Cisco Technical Assistance Center (TAC) oder die von ihnen beauftragten Wartungsfirmen wenden.

Erwerb fester Software

Cisco hat Software-Updates veröffentlicht, die diese Schwachstellen beheben. Vor der Bereitstellung der Software sollten Kunden ihren Wartungsanbieter konsultieren oder die Software auf Kompatibilität der Funktionssätze und auf bekannte umgebungsspezifische Probleme überprüfen.

Kunden dürfen nur die erworbenen Feature-Sets installieren und Unterstützung erwarten. Durch die Installation, das Herunterladen, den Zugriff auf oder die anderweitige Nutzung solcher Software-Upgrades erklären Kunden sich mit den Bestimmungen der Cisco Softwarelizenzbedingungen einverstanden, die unter http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html zur Verfügung stehen oder in den Cisco.com-Downloads unter http://www.cisco.com/public/sw-center/sw-usingswc.shtml aufgeführt sind.

Wenden Sie sich bei Software-Upgrades nicht an psirt@cisco.com oder security-alert@cisco.com.

Kunden mit Serviceverträgen

Kunden mit Verträgen sollten Software über ihre regelmäßigen Aktualisierungskanäle beziehen. Bei den meisten Kunden sollten Software-Patches und Bugfixes über das Software Center unter Cisco.com bezogen werden. Weitere Informationen finden Sie unter http://www.cisco.com/cisco/software/navigator.html.

Kunden, die Support-Organisationen von Drittanbietern verwenden

Kunden, deren Cisco Produkte im Rahmen von vorherigen oder bestehenden Vereinbarungen mit Drittanbieter-Supportorganisationen wie Cisco Partnern, autorisierten Resellern oder Service Providern bereitgestellt oder gewartet werden, sollten sich an diese Support-Organisation wenden, um Unterstützung bei der geeigneten Vorgehensweise in Bezug auf diese Beratung zu erhalten.

Die Effektivität von Problemumgehungen und Problembehebungen hängt von bestimmten Kundensituationen ab, z. B. Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischen Zielen. Aufgrund der Vielzahl der betroffenen Produkte und Versionen sollten sich Kunden mit ihrem Service Provider oder der Support-Organisation in Verbindung setzen, um sicherzustellen, dass jede angesetzte Problemumgehung oder -behebung für das beabsichtigte Netzwerk am besten geeignet ist, bevor sie bereitgestellt wird.

Kunden ohne Serviceverträge

Kunden, die direkt bei Cisco einkaufen, aber keinen Cisco Servicevertrag abgeschlossen haben, und Kunden, die über Drittanbieter einkaufen, jedoch keine fixe Software über ihren Verkaufsort erhalten, sollten Software-Patches und Fehlerbehebungen erhalten, indem sie sich an das Cisco Technical Assistance Center (TAC) wenden. Ansprechpartner beim TAC:

- +1 800 553 2447 (innerhalb Nordamerikas gebührenfrei)
- +1 408 526 7209 (gebührenpflichtiger Anruf von einem beliebigen Standort weltweit)
- E-Mail: tac@cisco.com

Kunden sollten ihre Produktseriennummer zur Verfügung stellen und darauf vorbereitet sein, die URL dieser Benachrichtigung als Nachweis für die Berechtigung zu einem Software-Patch oder einer Fehlerkorrektur anzugeben. Kunden ohne Servicevertrag sollten einen Software-Patch oder eine Fehlerbehebung über das TAC anfordern.

Unter http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html erhalten Sie weitere Kontaktinformationen des TAC, einschließlich lokalisierter Telefonnummern sowie Anleitungen und E-Mail-Adressen für die Verwendung in verschiedenen Sprachen.

Status dieser Mitteilung: Finale

Distribution

Diese Ankündigung kann auf der weltweiten Cisco Website unter folgender Adresse abgerufen werden:

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160323-bundle

Neben der weltweiten Veröffentlichung über das Internet ist eine Textversion dieser Benachrichtigung mit dem PSIRT PGP-Schlüssel von Cisco eindeutig signiert und wird an die folgenden E-Mail- und Usenet-Nachrichtenempfänger weitergeleitet.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- fulldisclosure@seclists.org
- comp.dcom.sys.cisco@newsgate.cisco.com

Künftige Aktualisierungen dieser Sicherheitsberatung werden, falls vorhanden, auf der weltweiten Cisco Website veröffentlicht, können jedoch in Mailinglisten oder Newsgroups aktiv angekündigt werden. Benutzer, die wegen dieses Problems besorgt sind, werden gebeten, die obige URL auf Updates zu überprüfen.

Revisionsverlauf

Cisco Sicherheitsverfahren

Umfassende Informationen zur Meldung von Sicherheitsschwachstellen in Cisco Produkten, zum Erhalten von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Cisco Website unter http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html. Dazu gehören auch Anweisungen für Presseanfragen zu Cisco Sicherheitsmitteilungen. Alle Cisco Sicherheitsempfehlungen finden Sie unter http://www.cisco.com/go/psirt.