Zusammenfassung der Cisco IOS- und IOS XE Software Security Advisory Bundled Publication, 26. September 2018

'+'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-20180926-Paket

https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20180926-bundle

Revision 1.0

Veröffentlichung 2018, 26. September 15:30 Uhr (GMT)

Inhalt

Zusammenfassung

Dieses Dokument ist Teil der Veröffentlichung der Cisco IOS- und IOS XE Software Security Advisory Bundled Publication am 26. September 2018, mit 12 Cisco Security Advisories, in denen 13 Sicherheitslücken beschrieben werden. Eine vollständige Liste der Ratgeber und Links zu diesen finden Sie unter Cisco Event Response: September 2018 Die Cisco IOS und IOS XE Software Security Advisory Bundled Publication.

Softwareversionen und -korrekturen

Bei der Erwägung von Software-Upgrades wird den Kunden empfohlen, sich regelmäßig mit den Ratgebern zu Cisco Produkten in Verbindung zu setzen, die auf der Seite "Cisco Security Advisories and Alerts" verfügbar sind, um Informationen zur Verfügbarkeit und eine vollständige Upgrade-Lösung zu erhalten.

In allen Fällen sollten Kunden sicherstellen, dass die zu aktualisierenden Geräte genügend Arbeitsspeicher enthalten und dass aktuelle Hardware- und Softwarekonfigurationen von der neuen Version weiterhin ordnungsgemäß unterstützt werden. 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 kostenlose Software-Updates veröffentlicht, die die in den Ratgebern beschriebenen Schwachstellen beheben. Kunden dürfen nur Softwareversionen und Funktionssätze installieren und unterstützen, für die sie eine Lizenz erworben haben. Durch die Installation, das Herunterladen, den Zugriff oder die anderweitige Nutzung solcher Software-Upgrades stimmen Kunden zu, die Bedingungen der Cisco Softwarelizenz zu befolgen: https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

Darüber hinaus dürfen Kunden Software nur herunterladen, für die sie eine gültige Lizenz besitzen, die direkt von Cisco oder über einen autorisierten Cisco Reseller oder Partner bezogen wird. In den meisten Fällen handelt es sich dabei um ein Wartungs-Upgrade für die zuvor erworbene Software. Kostenlose Sicherheits-Software-Updates berechtigen Kunden nicht zu einer neuen Softwarelizenz, zusätzlichen Software-Feature-Sets oder umfangreichen Upgrades der Version.

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-Upgrades über das Software Center auf Cisco.com bezogen werden.

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 die Ratgeber 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, aber keine fest installierte Software über ihren Verkaufsort erwerben können, sollten Upgrades erhalten, indem Sie sich an das Cisco Technical Assistance Center (TAC) wenden: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Kunden sollten über die Produktseriennummer verfügen und bereit sein, die URL dieses Dokuments als Nachweis für die Berechtigung zu einem kostenlosen Upgrade anzugeben.

Status dieser Mitteilung: Finale

Distribution

Dieses Dokument ist unter dem folgenden Link verfügbar:
https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20180328-bundle

Künftige Aktualisierungen dieses Dokuments werden, falls vorhanden, auf der vorherigen URL veröffentlicht, können aber nicht aktiv auf Mailinglisten angekündigt werden. Benutzer werden gebeten, die vorangehende URL auf Updates zu überprüfen.

Informationen zum Erhalt von Informationen zu Sicherheitslücken von Cisco finden Sie in der Cisco Security Vulnerability Policy.

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 in den Cisco Security Vulnerability Policy. Dazu gehören auch Anweisungen für Presseanfragen zu Cisco Sicherheitslücken. Alle Cisco Security Advisories finden Sie unter https://www.cisco.com/go/psirt.