

Zusammenfassung der Cisco IOS- und IOS XE Software Security Advisory Bundled Publication, 22. März 2017

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

'); } function startExpandIndentSubheader() { document.write('

'); } function endExpandIndentSubheader() { document.write('

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

'+'+'[Expand all sections](#)'+' '+'[Collapse all sections](#)'+'+'[Close Section](#)'+'

Beratungs-ID: cisco-sa-20170322-Paket

<https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20170322-bundle>

Revision 1.0

Für die Veröffentlichung 2017, 22. März, 16:00 Uhr UTC (GMT)

Inhalt

[Zusammenfassung](#)

[Softwareversionen und -korrekturen](#)

[Erwerb fester Software](#)

[Status dieser Mitteilung: Finale](#)

[Distribution](#)

[Revisionsverlauf](#)

[Cisco Sicherheitsverfahren](#)

[Zusammenfassung](#)

Dieses Dokument ist Teil der Veröffentlichung der Cisco IOS- und IOS XE Software Security Advisory Bundled Publication am 22. März 2017, mit fünf Cisco Security Advisories, die fünf Sicherheitslücken beschreiben. Eine vollständige Liste der Ratgeber und Links zu diesen finden Sie unter [Cisco Event Response: März 2017 Veröffentlichung der Cisco IOS- und IOS XE Software Security Advisory-Pakete](#).

[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 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:

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.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. Für die meisten Kunden sollten Software-Upgrades über das Software Center auf der weltweiten Cisco Website unter <http://www.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 Problembhebungen 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:

http://www.cisco.com/en/US/support/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

DIESES DOKUMENT WIRD "WIE BESEHEN" BEREITGESTELLT UND IMPLIZIERT KEINE GEWÄHRLEISTUNG ODER GEWÄHRLEISTUNG, EINSCHLIESSLICH DER GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT ODER EIGNUNG FÜR EINE BESTIMMTE VERWENDUNG. DIE VERWENDUNG DER INFORMATIONEN IN DEN DOKUMENTEN ODER MATERIALIEN, DIE IM DOKUMENT VERKNÜPFT SIND, ERFOLGT AUF EIGENES RISIKO. CISCO BEHÄLT SICH DAS RECHT VOR, DIESES DOKUMENT JEDERZEIT ZU ÄNDERN ODER ZU AKTUALISIEREN.

Eine eigenständige Kopie oder Umschreibung des Textes dieses Dokuments, bei der die Distributions-URL ausgelassen wird, ist eine unkontrollierte Kopie, bei der wichtige Informationen fehlen oder sachliche Fehler auftreten können. Die Informationen in diesem Dokument sind für Endbenutzer von Cisco Produkten bestimmt.

Distribution

Dieses Dokument ist auf der weltweiten Cisco Website unter folgender Adresse verfügbar:

<https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20170322-bundle>

Neben der weltweiten Veröffentlichung über das Internet ist eine Textversion dieses Dokuments mit dem PSIRT-PGP-Schlüssel von Cisco eindeutig signiert und an die folgenden E-Mail- und Usenet-Nachrichtenempfänger gesendet:

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Künftige Aktualisierungen dieses Dokuments werden, falls vorhanden, auf der weltweiten Cisco Website veröffentlicht, können aber auch aktiv in Mailinglisten oder Newsgroups veröffentlicht 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/c/en/us/about/security-center/security-vulnerability-policy.html>. Dazu gehören auch Anweisungen für Presseanfragen zu Cisco Sicherheitslücken. Alle Cisco Security Advisories finden Sie unter <http://www.cisco.com/go/psirt>.