

Identifizieren und Eindämmen der Sicherheitslücke bei den Standard-Anmeldeinformationen der Cisco Identity Services Engine-Datenbank

Identifizieren und Eindämmen der Sicherheitslücke bei den Standard-Anmeldeinformationen der Cisco Identity Services Engine-Datenbank

Beratungs-ID: cisco-amb-20110920-ise

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110920-ise>

Version 1.1

Zuletzt aktualisiert am 20. Oktober 2011 um 13:58 Uhr (GMT)

Zur öffentlichen Veröffentlichung 2011 September 20 16:00 UTC (GMT)

Inhalt

[Antwort von Cisco](#)

[Gerätespezifische Eindämmung und Identifizierung](#)

[Zusätzliche Informationen](#)

[Revisionsverlauf](#)

[Cisco Sicherheitsverfahren](#)

[Zugehörige Informationen](#)

Antwort von Cisco

Dieses "Applied Mitigation Bulletin" ist ein Begleitdokument zur Schwachstelle mit den Standard-Anmeldedaten der Cisco Identity Services Engine für die PSIRT-Sicherheitsberatung und bietet Identifizierungs- und Eindämmungstechniken, die Administratoren auf Cisco Netzwerkgeräten einsetzen können.

Merkmale der Schwachstelle

Im Lieferumfang der Cisco Identity Services Engine (ISE) sind drei Standardanmeldeinformationen

(Kombinationen aus Benutzername und Kennwort) für die zugrunde liegende Datenbank enthalten. Ein entfernter Angreifer könnte diese Anmeldeinformationen nutzen, um die Gerätekonfiguration und -einstellungen zu ändern oder eine vollständige administrative Kontrolle über das Gerät zu erlangen. Diese Schwachstelle kann per Remote-Zugriff mit Authentifizierung und ohne Benutzereingriff ausgenutzt werden. Der Angriffsvektor für die Ausnutzung erfolgt über Oracle SQL*Net-Pakete, die den TCP-Port 1521 verwenden.

Dieser Schwachstelle wurde der CVE-Identifizierer CVE-2011-3290 zugewiesen.

Überblick über Sicherheitslücken

Informationen zu anfälliger, nicht betroffener und fest installierter Software finden Sie in der PSIRT-Sicherheitsberatung, die unter folgendem Link verfügbar ist:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110920-ise>.

Überblick über die Risikominderungstechnik

Cisco Geräte bieten verschiedene Gegenmaßnahmen für diese Schwachstelle. 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 von Transit-Zugriffskontrolllisten (tACLs) effektive Möglichkeiten zur Verhinderung von Exploits. Dieser Schutzmechanismus filtert und löscht Pakete, die versuchen, diese Schwachstelle auszunutzen.

Eine effektive Exploit-Abwehr kann auch durch die Cisco Adaptive Security Appliance der Serie ASA 5500, das Firewall Services Module (FWSM) für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 sowie das Adaptive Security Appliance Service Module (ASASM) mit tACLs erreicht werden. Dieser Schutzmechanismus filtert und löscht Pakete, die versuchen, diese Schwachstelle auszunutzen.

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

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

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

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

Risikomanagement

Den Unternehmen wird empfohlen, die potenziellen Auswirkungen dieser Schwachstelle 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 jeder 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: 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 Transit-Zugriffskontrolllisten (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 dieser Schwachstelle bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die tACL-Richtlinie verweigert nicht autorisierte SQL*Net-Pakete auf dem TCP-Port 1521, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.60.0/24 der IP-Adressraum, der von den betroffenen ISE-Geräten verwendet wird. Der Host unter 192.168.100.1 gilt als vertrauenswürdige ISE-Quelle, die Zugriff auf die betroffenen ISE-Geräte benötigt. 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 to the affected ISE device on the vulnerable port! access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1521 !-- The following vulnerability-specific access control entry !-- (ACE) can aid in identification of attacks! access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 1521 !-- 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 150 deny ip any any !-- Apply tACL to interfaces in the ingress direction! interface GigabitEthernet0/0 ip access-group 150 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 unreachable** deaktiviert werden. Die Durchsatzbegrenzung "ICMP unreachable" kann mithilfe des globalen Konfigurationsbefehls **ip icmp rate-limit unreachable interval-in-ms** vom Standardwert geändert werden.

Identifizierung: Transit-Zugriffskontrolllisten

Nachdem der Administrator die tACL auf eine Schnittstelle angewendet hat, identifiziert der Befehl **show ip access-lists** die Anzahl der SQL*Net-Pakete auf dem TCP-Port 1521, die gefiltert wurden. Den Administratoren wird empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen. Beispielausgabe für **show ip access-lists 150** folgt:

```
router#show ip access-lists 150
Extended IP access list 150
 10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1521
 20 deny tcp any 192.168.60.0 0.0.0.255 eq 1521 (7 matches)
 30 deny ip any any
router#
```

Im vorherigen Beispiel hat die Zugriffsliste 150 7 SQL*Net-Pakete auf dem TCP-Port 1521 für die Zugriffskontrolllisteneintragszeile (ACE) 20 verworfen.

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 bestimmten ACEs entsprechen. 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.

Bei Cisco IOS-Software kann der Befehl **ip access-list logging interval 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.

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, bei denen möglicherweise versucht wird, die Schwachstelle auszunutzen. Den Administratoren wird empfohlen, Datenflüsse zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, die Schwachstelle auszunutzen, oder ob es sich um legitime Datenflüsse handelt.

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 4456704 bytes
 1885 active, 63651 inactive, 59960004 added
129803821 age polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
 0 active, 16384 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 | Flows /Sec | Packets /Flow | Bytes /Pkt | Packets /Sec | Active(Sec) /Flow | Idle(Sec) /Flow |
|------------|-------------|------------|---------------|------------|--------------|-------------------|-----------------|
| TCP-Telnet | 11393421 | 2.8 | 1 | 48 | 3.1 | 0.0 | 1.4 |
| TCP-FTP | 236 | 0.0 | 12 | 66 | 0.0 | 1.8 | 4.8 |
| TCP-FTPD | 21 | 0.0 | 13726 | 1294 | 0.0 | 18.4 | 4.1 |
| TCP-WWW | 22282 | 0.0 | 21 | 1020 | 0.1 | 4.1 | 7.3 |
| TCP-X | 719 | 0.0 | 1 | 40 | 0.0 | 0.0 | 1.3 |
| TCP-BGP | 1 | 0.0 | 1 | 40 | 0.0 | 0.0 | 15.0 |
| TCP-Frag | 70399 | 0.0 | 1 | 688 | 0.0 | 0.0 | 22.7 |
| TCP-other | 47861004 | 11.8 | 1 | 211 | 18.9 | 0.0 | 1.3 |
| UDP-DNS | 582 | 0.0 | 4 | 73 | 0.0 | 3.4 | 15.4 |
| UDP-NTP | 287252 | 0.0 | 1 | 76 | 0.0 | 0.0 | 15.5 |
| UDP-other | 310347 | 0.0 | 2 | 230 | 0.1 | 0.6 | 15.9 |
| ICMP | 11674 | 0.0 | 3 | 61 | 0.0 | 19.8 | 15.5 |
| IPv6INIP | 15 | 0.0 | 1 | 1132 | 0.0 | 0.0 | 15.4 |
| GRE | 4 | 0.0 | 1 | 48 | 0.0 | 0.0 | 15.3 |
| Total: | 59957957 | 14.8 | 1 | 196 | 22.5 | 0.0 | 1.5 |

| SrcIf | SrcIPAddress | DstIf | DstIPAddress | Pr | SrcP | DstP | Pkts |
|--------------|-----------------------|--------------|-----------------------|-----------|-------------|-------------|----------|
| Gi0/0 | 192.168.10.201 | Gi0/1 | 192.168.60.102 | 06 | 0984 | 05F1 | 1 |
| Gi0/0 | 192.168.11.54 | Gi0/1 | 192.168.60.158 | 06 | 0911 | 05F1 | 3 |
| Gi0/1 | 192.168.150.60 | Gi0/0 | 10.89.16.226 | 06 | 0016 | 12CA | 1 |
| Gi0/0 | 192.168.13.97 | Gi0/1 | 192.168.60.28 | 06 | 0B3E | 05F1 | 5 |
| Gi0/0 | 192.168.10.17 | Gi0/1 | 192.168.60.97 | 06 | 0B89 | 05F1 | 1 |

```

Gi0/0      10.88.226.1      Gi0/1      192.168.202.22  11 007B 007B      1
Gi0/0      192.168.12.185  Gi0/1      192.168.60.239  06 0BD7 05F1      1
Gi0/0      10.89.16.226    Gi0/1      192.168.150.60  06 12CA 0016      1
router#

```

Im vorherigen Beispiel gibt es mehrere Datenflüsse für **SQL*Net** auf dem **TCP-Port 1521** (**Hexadezimalwert 05F1**).

Um nur die Datenverkehrsflüsse für SQL*Net-Pakete auf dem TCP-Port 1521 (Hexadezimalwert 05F1) anzuzeigen, zeigt der Befehl **den IP-Cache-Fluss an. | include SrcIf|_06_.*05F1** zeigt die zugehörigen TCP NetFlow-Datensätze wie folgt an:

TCP-Flows

```

router#show ip cache flow | include SrcIf|_06_.*05F1
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP      Pkts
Gi0/0      192.168.10.201    Gi0/1      192.168.60.102    06 0984 05F1      1
Gi0/0      192.168.11.54     Gi0/1      192.168.60.158    06 0911 05F1      3
Gi0/0      192.168.13.97     Gi0/1      192.168.60.28     06 0B3E 05F1      5
Gi0/0      192.168.10.17     Gi0/1      192.168.60.97     06 0B89 05F1      1
Gi0/0      192.168.12.185    Gi0/1      192.168.60.239    06 0BD7 05F1      1
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 dieser Schwachstelle bieten, wenn der Angriff von einer vertrauenswürdigen Quelladresse ausgeht.

Die tACL-Richtlinie verweigert nicht autorisierte SQL*Net-Pakete auf dem TCP-Port 1521, die an betroffene Geräte gesendet werden. Im folgenden Beispiel ist 192.168.60.0/24 der IP-Adressraum, der von den betroffenen ISE-Geräten verwendet wird. Der Host unter 192.168.100.1 gilt als vertrauenswürdige ISE-Quelle, die Zugriff auf die betroffenen ISE-Geräte benötigt. 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 port! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 1521 !-- The following vulnerability-
specific access control entry !-- (ACE) can aid in identification of attacks! access-
list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 1521 !-- 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

```

Identifizierung: Transit-Zugriffskontrolllisten

Nachdem die tACL auf eine Schnittstelle angewendet wurde, können Administratoren mit dem Befehl **show access-list** die Anzahl der SQL*Net-Pakete auf dem TCP-Port 1521 identifizieren, die gefiltert wurden. Den Administratoren wird empfohlen, gefilterte Pakete zu untersuchen, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen.

Beispielausgabe für **show access-list tACL-Policy**:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
    192.168.60.0 255.255.255.0 eq sqlnet (hitcnt=29)
access-list tACL-Policy line 2 extended deny tcp any
    192.168.60.0 255.255.255.0 eq sqlnet (hitcnt=37)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=94)
firewall#
```

Im vorherigen Beispiel hat die Zugriffsliste *tACL-Policy* **37 SQL*Net-Pakete** auf dem **TCP-Port 1521** verworfen, die von einem nicht vertrauenswürdigen Host oder Netzwerk empfangen wurden. Darüber hinaus kann die Syslog-Meldung *106023* nützliche Informationen bereitstellen, z. B. die Quell- und Ziel-IP-Adresse, die Quell- und Ziel-Port-Nummern und das IP-Protokoll für das abgelehnte Paket.

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 kein **log-**Schlüsselwort 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 beschriebene Schwachstelle 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
Sep 20 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
    dst inside:192.168.60.191/1521 by access-group "tACL-Policy"
Sep 20 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
    dst inside:192.168.60.33/1521 by access-group "tACL-Policy"
Sep 20 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
    dst inside:192.168.60.240/1521 by access-group "tACL-Policy"
firewall#
```

Im vorherigen Beispiel zeigen die für die *tACL-tACL-Richtlinie* protokollierten Nachrichten

SQL*Net-Pakete für den TCP-Port 1521 an, die an den Adressblock gesendet wurden, 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.

[Cisco Intrusion Prevention System](#)

Eindämmung: Cisco IPS-Signaturereignisaktionen

Administratoren können Cisco Intrusion Prevention System (IPS)-Appliances und -Servicemodule verwenden, um eine Erkennung von Sicherheitsrisiken zu ermöglichen und Versuche zu verhindern, die in diesem Dokument beschriebene Schwachstelle auszunutzen. Beginnend mit dem Signatur-Update S596 für Sensoren, auf denen Cisco IPS 6.x und höher ausgeführt wird, kann die Schwachstelle mit der Signatur 39226/0 erkannt werden (Signature Name: Cisco Identity Services Engine Database Default Credentials Vulnerability). Signatur 39226/0 ist standardmäßig aktiviert, löst ein Ereignis mit *mittlerem* Schweregrad aus, hat eine Signatortreue-Bewertung (SFR) von 85 und wird mit der Standardereignisaktion **product-alert** konfiguriert.

Signatur 39226/0 wird ausgelöst, wenn ein Versuch erkannt wird, eine Schwachstelle in der Cisco Identity Services Engine-Datenbank auszunutzen. Wenn diese Signatur ausgelöst wird, kann dies auf einen potenziellen Angriff auf die Schwachstelle hinweisen.

Hinweis: Diese Signatur kann eine ordnungsgemäße Warnung ausgeben, wenn das Produkt in einer verteilten Umgebung bereitgestellt wird. Es wird empfohlen, die Signatur in solchen Situationen zu deaktivieren.

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 beschriebene Schwachstelle 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 beschriebene Schwachstelle auszunutzen. Der Schutz vor Bedrohungen wird durch eine Standardüberschreibung erreicht, die eine Ereignisaktion für ausgelöste Signaturen mit einem *riskRatingValue* größer 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 Incidents zu Ereignissen erstellen, die mit der in diesem Dokument beschriebenen Schwachstelle zusammenhängen. Hierzu wird die IPS-Signatur 39226/0 (Signature Name: Cisco Identity Services Engine Database Default Credentials Vulnerability) verwendet. Nachdem das dynamische Signatur-Update S596 heruntergeladen wurde, wird mit dem Schlüsselwort **NR-39226/0** für die IPS-Signatur 39226/0 und dem Abfragetyp **Alle übereinstimmenden Ereignis-Rohmeldungen** auf der Cisco Security MARS-Appliance ein Bericht bereitgestellt, in dem die durch die IPS-Signatur erstellten Vorfälle aufgelistet werden.

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 Signaturaktualisierungen konfiguriert sind, 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 Wert für die *IPS-Signaturversion* 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 | 20. Oktober 2011 | Tabelle im Revisionsverlauf korrigiert |
| Version 1.0 | 20. September 2011 | Erste öffentliche 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 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](#)
- [Gegenmaßnahmen für die böswillige Verwendung von IPv6-Typ-0-Routing-Headern](#)
- [Cisco Firewall-Produkte - Startseite auf Cisco.com](#)
- [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.