[NEWS] Cisco OpenSSL Implementation Vulnerability

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2004−03/0052.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 03/17/04

```
To: list@securiteam.com
Date: 17 Mar 2004 18:57:29 +0200
```

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: http://www.securiteam.com
− − promotion

The SecuriTeam alerts list − Free, Accurate, Independent.

Get your security news from a reliable source.
http://www.securiteam.com/mailinglist.html

− − − − − − − − −

Cisco OpenSSL Implementation Vulnerability
−−−

vulnerable for the Cisco Catalyst 6500 Series and Cisco 7600 Series Routers.
* Cisco PIX Firewall
* Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers
* Cisco MDS 9000 Series Multilayer Switch
* Cisco Content Service Switch (CSS) 11000 series
* Cisco Global Site Selector (GSS) 4480
* CiscoWorks Common Services (CWCS) version 2.2 and CiscoWorks Common Management Foundation (CMF) version 2.1
* Cisco Access Registrar (CAR)

The following products have their SSL implementation based on the OpenSSL code and are not affected by this vulnerability.
* Cisco Secure Intrusion Detection System (NetRanger) appliance. This includes the IDS−42xx appliances, NM−CIDS and WS−SVS−IDSM2.
* Cisco SN 5428 and SN 5428−2 Storage Router
* Cisco CNS Configuration Engine
* Cisco Network Analysis Modules (NAM) for the Cisco Catalyst 6000 and 6500 Series switches and Cisco 7600 Series routers
* Cisco SIP Proxy Server (SPS)
* CiscoWorks 1105 Hosting Solution Engine (HSE)
* CiscoWorks 1105 Wireless LAN Solution Engine (WLSE)
* Cisco Ethernet Subscriber Solution Engine (ESSE)

The following products, which implement SSL, are not affected by this vulnerability.
* Cisco VPN 3000 Series Concentrators

CatOS does not implement SSL and is not vulnerable.

No other Cisco products are currently known to be affected by this vulnerability. This vulnerability is still being actively investigated across Cisco products and status of some products has still not been determined.

Details:
Secure Sockets Layer (SSL), is a protocol used to encrypt the data transferred over an TCP session. SSL in Cisco products is mainly used by the HyperText Transfer Protocol Secure (HTTPS) web service for which the default TCP port is 443. The affected products, listed above, are only vulnerable if they have the HTTPS service enabled and the access to the service is not limited to trusted hosts or network management workstations.

To check if the HTTPS service is enabled one can do the following:
1. Check the configuration on the device to verify the status of the HTTPS service.
2. Try to connect to the device using a standard web browser that supports SSL using a URL similar to https://ip_address_of_device/.
3. Try and connect to the default HTTPS port, TCP 443, using Telnet.

telnet ip_address_of_device 443. If the session connects the service is enabled and accessible.

Testing by the OpenSSL development team has uncovered a null−pointer assignment in the do_change_cipher_spec() function. A remote attacker could perform a carefully crafted SSL/TLS handshake against a server that used the OpenSSL library in such a way as to cause OpenSSL to crash. This crash on many Cisco products would cause the device to reload. Repeated exploitation of this vulnerability would result in a Denial of Service (DoS) attack on the device.

Another flaw was also discovered in the SSL/TLS handshaking code when using Kerberos ciphersuites. A remote attacker could perform a carefully crafted SSL/TLS handshake against a server configured to use Kerberos ciphersuites in such a way as to cause OpenSSL to crash. None of the Cisco OpenSSL implementations are known to use Kerberos ciphersuites and are therefore not affected by this second vulnerability.

A third vulnerability described in the NISCC advisory is a bug in older versions of OpenSSL, versions before 0.9.6d that can also lead to a Denial of Service attack. None of the Cisco OpenSSL implementations are known to be affected by this older OpenSSL issue.

More information on the OpenSSL vulnerability is available at <http://www.openssl.org/news/secadv_20040317.txt> http://www.openssl.org/news/secadv_20040317.txt.

* Cisco IOS − All 12.1(11)E and later IOS software crypto (56i and k2) image releases in the 12.1E release train for the Cisco 7100 and 7200 Series Routers are affected by this vulnerability. All IOS software crypto (k8, k9, and k91) image releases in the 12.2SY release train for the Cisco Catalyst 6500 Series and Cisco 7600 Series Routers are affected by this vulnerability. The SSH implementation in IOS is not dependent on any OpenSSL code. SSH implementations in IOS do not handle certificates, yet, and therefore do not use any SSL code for SSH. OpenSSL in 12.1E and 12.2SY release trains is only used for providing the HTTPS and VPN Device Manager (VDM) services. This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCee00041. The HTTPS web service, that uses the OpenSSL code, on the device is disabled by default. The no ip http secure−server command may be used to disable the HTTPS web service on the device, if! required. The SSH and IPSec services in IOS are not vulnerable to this vulnerability.

* Cisco PIX Firewall − PIX 6.x releases are affected by this vulnerability. PIX 5.x releases do not contain any SSL code and are not vulnerable. This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCed90672.

* Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers − This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCee02055.

* Cisco MDS 9000 Series Multilayer Switches − This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCed96246.

* Cisco Content Service Switch (CSS) 11000 series − WebNS version 6.x and 7.x are affected by this vulnerability. WebNS version 5.x is not vulnerable to the OpenSSL vulnerabilities. This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCee01234 for SCM and is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCee01240 for the SSL module.

* Cisco Global Site Selector (GSS) 4480 − This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCee01057.

* CiscoWorks Common Services (CWCS) version 2.2 and CiscoWorks Common Management Foundation (CMF) version 2.1 − This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCsa13748.

* Cisco Access Registrar (CAR) − This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCee01956.

The Internetworking Terms and Cisco Systems Acronyms online guides can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/> http://www.cisco.com/univercd/cc/td/doc/cisintwk/.

Impact:
An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack.

Software Versions and Fixes:
* Cisco IOS −

Release	Train	Fixed Releases	Availability
12.2SY	12.2(14)SY4	March 25	
12.1E	12.1(13)E14	April 8	
12.1.(19)E7	April 8		
12.1(20)E3	April 26		

* Cisco PIX Firewall − The vulnerability is fixed in software releases 6.0(4)102, 6.1(5)102, 6.2(3)107, and 6.3(3)124. These engineering builds may be obtained by contacting the Cisco Technical Assistance Center (TAC). TAC Contact information is given in the Obtaining Fixed Software section below.

* Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers − The vulnerability is fixed in software release 1.1.3(14) which will be available by Monday, 22 of March, 2004. This engineering builds may be obtained by contacting the Cisco Technical Assistance Center (TAC). TAC Contact information is given in the Obtaining Fixed Software section below.

* Cisco MDS 9000 Series Multilayer Switches − No fixed software release or software availability date has been determined yet.

* Cisco Content Service Switch (CSS) 11000 series −No fixed software release or software availability date has been determined yet.

* Cisco Global Site Selector (GSS) 4480 − No fixed software release or software availability date has been determined yet.

* CiscoWorks Common Services (CWCS) version 2.2 and CiscoWorks Common Management Foundation (CMF) version 2.1 − No fixed software release or software availability date has been determined yet.

* Cisco Access Registrar (CAR) − The vulnerability is fixed in software release 3.5.0.12 which will be available by Friday, 26 of March, 2004.

Obtaining Fixed Software:
Cisco is offering free software upgrades to address this vulnerability for all affected customers.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, Customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw−license−agreement.html> http://www.cisco.com/public/sw−license−agreement.html, or as otherwise set forth at the Cisco Connection Online Software Center at <http://www.cisco.com/public/sw−center/sw−usingswc.shtml> http://www.cisco.com/public/sw−center/sw−usingswc.shtml.

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com/tacpage/sw−center> http://www.cisco.com/tacpage/sw−center. To access the software download URL, you must be a registered user and you must be logged in.

Customers whose Cisco products are provided or maintained through a prior or existing agreement with third−party support organizations such as Cisco Partners, authorized resellers, or service providers, should contact that support organization for assistance with obtaining the software upgrade(s).

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third−party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC) using the contact information listed below. In these cases, customers are entitled to obtain a free upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (noted above).

Cisco TAC contacts are as follows:

* +1 800 553 2447 (toll free from within North America)
* +1 408 526 7209 (toll call from anywhere in the world)
* e−mail: tac@cisco.com

See <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml for additional
TAC contact information, including special localized telephone numbers and
instructions and e−mail addresses for use in various languages.

Please have your product serial number available and give the URL of this
notice as evidence of your entitlement to a upgrade. Upgrades for
non−contract customers must be requested through the TAC.

Please do not contact either "psirt@cisco.com" or
"security−alert@cisco.com" for software upgrades.

Workarounds:
The Cisco PSIRT recommends that affected users upgrade to a fixed software
version of code as soon as it is available.

* Restrict access to the HTTPS server on the network device. Allow access
to the network device only from trusted workstations by using access lists
/ MAC filters that are available on the affected platforms.

* Disable the SSL server / service on the network device. This workaround
must be weighed against the need for secure communications with the
vulnerable device.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco
Systems Product Security Incident Response Team.

The original article can be found at:
<http://www.cisco.com/warp/public/707/cisco−sa−20040317−openssl.shtml>
http://www.cisco.com/warp/public/707/cisco−sa−20040317−openssl.shtml

==========

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list−unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list−subscribe@securiteam.com

==========
==========

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.