Cisco Security Advisory

OpenSSL RSA Temporary Key Cryptographic Downgrade Vulnerability

Advisory ID: Cisco-SA-20150113-CVE-2015-0204
Last Updated: 2015 September 25 12:45 GMT
Published: 2015 January 13 19:57 GMT
Version14.0: Final
CVSS Score: Base - 5.0
Workarounds: See below
Cisco Bug IDs: CSCum57065 CSCus42699 CSCus42701 CSCus42702 CSCus42705 CSCus42706 CSCus42709 CSCus42710 CSCus42711 CSCus42712 CSCus42713 CSCus42721 CSCus42723 CSCus42724 CSCus42726 CSCus42727 CSCus42732 CSCus42737 CSCus42738 CSCus42739 CSCus42742 CSCus42748 CSCus42749 CSCus42751 CSCus42752 CSCus42753 CSCus42754 CSCus42755 CSCus42758 CSCus42763 CSCus42766 CSCus42768 CSCus42772 CSCus42775 CSCus42781 CSCus42785 CSCus42786 CSCus42787 CSCus42791 CSCus42792 CSCus42800 CSCus42801 CSCus42804 CSCus42812 CSCus42814 CSCus42816 CSCus42818 CSCus42821 CSCus42827 CSCus42828 CSCus42829 CSCus42831 CSCus42833 CSCus42834 CSCus42836 CSCus42840 CSCus42850 CSCus42851 CSCus42853 CSCus42879 CSCus42883 CSCus42900 CSCus42901 CSCus42904 CSCus42906 CSCus42908 CSCus42917 CSCus42952 CSCus42954 CSCus42958 CSCus42966 CSCus42967 CSCus42968 CSCus42972 CSCus42982 CSCus42983 CSCus42996 CSCus43000 CSCus43003 CSCus43015 CSCus43016 CSCus43020 CSCus43022 CSCus43041 CSCus43052 CSCus44478 CSCus60116 CSCus61884 CSCus77211 CSCut14256 CSCut82321

CVE-2015-0204
CWE-310

Download CVRF

Download PDF

Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

IS OpenSSL RSA Temporary Key Cryptographic Downgrade Vulnerability

ST 33686
ST 33687
ST 33688
ST 33689
ST 33690
ST 33691
ST 33692
ST 33693
ST 33694
ST 33695
ST 33696
ST 33697
ST 33698
ST 33699
ST 33700
ST 33701
ST 33702
ST 33703
ST 33777
ST 33778
ST 33779
ST 33780
ST 33781
ST 33782
ST 33783
ST 33784
ST 33785
ST 33786
ST 33787
ST 33788
ST 33789
ST 33790
ST 33791
ST 33792
ST 33793
ST 33794
ST 33795
ST 33796
ST 33797
ST 33798
ST 33799
ST 33800
ST 33801
ST 33802
ST 33803
ST 33804

Summary

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to bypass security restrictions.

The vulnerability is due to improper handling of an RSA temporary key. An attacker with a privileged network position could exploit the vulnerability by returning a weak temporary RSA key to a system using an application that uses the vulnerable OpenSSL library. When processed, the insecure temporary key could result in reduced cryptographic protections, which could allow the attacker to bypass security protections.

OpenSSL has confirmed the vulnerability and released software updates.

To exploit the vulnerability, the attacker likely requires privileged network access to trusted or internal networks to return temporary RSA keys to the targeted system. This access requirement greatly limits the likelihood of a successful exploit.

Affected Products

OpenSSL has released a security advisory at the following link: CVE-2015-0204

BlackBerry has released a security advisory at the following link: CVE-2015-0204

FreeBSD has released a VuXML document at the following link: OpenSSL -- multiple vulnerabilities

HP has released security bulletins c04604357, c04635715, c0467933, c04765169, c04762744, c04773241, c04765115, c04774021 and c04805275 at the following links: HPSBGN03299 SSRT101987, HPSBOV03318, HPSBUX03334 SSRT102000, HPSBMU03397 SSRT102192, HPSBMU03394 SSRT102187, HPSBMU03345 SSRT102095, HPSBMU03413, HPSBMU03396 and HPSBMU03422 SSRT101438

IBM has released a security advisory at the following link: CVE-2015-0204

Red Hat has released an official CVE statement and security advisories for bug 1180184 at the following links: CVE-2015-0204, RHSA-2015:0066 and RHSA-2015:0849

Splunk has released a security advisory at the following link: SP-CAAANZ7

Vulnerable Products

The following OpenSSL versions are vulnerable:

- OpenSSL versions prior to 1.0.1k
- OpenSSL versions prior to 1.0.0p
- OpenSSL versions prior to 0.9.8zd

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Workarounds

Administrators are advised to apply the appropriate updates.

Administrators are advised to allow only trusted users to have network access.

Administrators are advised to monitor affected systems.

Fixed Software

OpenSSL has released updated software at the following links:

For OpenSSL 1.0.1
OpenSSL 1.0.1k

For OpenSSL 1.0.0
OpenSSL 1.0.0p

For OpenSSL 0.9.8
OpenSSL 0.9.8zd

BlackBerry customers are advised to follow the resolution steps mentioned in the vendor advisory to mitigate this vulnerability.

CentOS packages can be updated using the **up2date** or **yum** command.

FreeBSD has released ports collection updates at the following link: Ports Collection Index

HP has released updated software for customers as described in the "Resolution" section of the security bulletin.

HP has released updated software at the following links:

HP Version Control Agent (VCA) 7.3.5
For Windows - X86
For Windows - X64
For Linux

HP Systems Insight Manager version 7.5.0

- for Linux for x86
- for MS Window

HP Version Control Repository Manager (VCRM) version 7.5.0

- For Windows
- For Linux

HP System Management Homepage version 7.2.6 for Windows 2003

IBM users are advised to follow the steps mentioned in the solutions section of the advisory to apply the fixes.

Red Hat has released updated software for registered subscribers at the following link: Red Hat Network. Red Hat packages can be updated on Red Hat Enterprise Linux versions 5 and later using the **yum** tool.

Splunk Enterprise has released updated software at the following links:

- Splunk Enterprise 6.2.3
- Splunk Light 6.2.3

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150113-CVE-2015-0204

Revision History

Version	Description	Section	Status	Date
13.0	HP has released additional security bulletins and software updates to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Aug-25
12.0	HP has released an additional security bulletin and software updates to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Aug-21
11.0	HP has released an additional security bulletin and software updates to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Aug-20
10.0	HP has released an additional security bulletin and software updates to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-May-21
9.0	Splunk has released released a advisory and updated software to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-May-06
8.0	Red Hat has released an additional security advisory and updated packages to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Apr-17
7.0	CentOS has released additional updated packages to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Apr-15
6.0	HP has released an additional security bulletin and updated software to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Apr-14
5.0	BlackBerry has released a security advisory and updated software to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Apr-03
4.0	HP has released a security bulletin and updated software to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Mar-30
	IBM has released a security			

3.0	advisory and fixes to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability.	NA	Final	2015-Feb-06
2.0	Red Hat has released a security advisory and updated packages to address the OpenSSL RSA temporary key cryptographic downgrade vulnerability. CentOS has also released updated packages to address this vulnerability.	NA	Final	2015-Jan-21

Legal Disclaimer