# CVE-2014-0160

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-0160 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2014-04-07 22:55:00 UTC |
| **Updated** | 2023-11-07 02:18:00 UTC |
| **Description** | The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension pa |

## Risk And Classification

**EPSS:** 0.944640000 probability, percentile 0.999950000 (date 2026-04-01)

**CISA KEV:** Listed on 2022-05-04; due 2022-05-25; ransomware use Unknown

**Problem Types:** CWE-125

## CISA Known Exploited Vulnerability

| | |
|---|---|
| **Vendor** | OpenSSL |
| **Product** | OpenSSL |
| **Name** | OpenSSL Information Disclosure Vulnerability |
| **Required Action** | Apply updates per vendor instructions. |
| **Notes** | https://nvd.nist.gov/vuln/detail/CVE-2014-0160 |

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 13.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 13.10 | All | All | All |
| Operating System | Debian | Debian Linux | 6.0 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 6.0 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 19 | All | All | All |
| Operating System | Fedoraproject | Fedora | 20 | All | All | All |
| Operating System | Fedoraproject | Fedora | 19 | All | All | All |
| Operating System | Fedoraproject | Fedora | 20 | All | All | All |
| Application | Filezilla-project | Filezilla Server | All | All | All | All |
| Application | Filezilla-project | Filezilla Server | All | All | All | All |
| Hardware | Intellian | V100 | - | All | All | All |
| Hardware | Intellian | V100 | - | All | All | All |
| Operating System | Intellian | V100 Firmware | 1.20 | All | All | All |
| Operating System | Intellian | V100 Firmware | 1.21 | All | All | All |
| Operating System | Intellian | V100 Firmware | 1.24 | All | All | All |
| Operating System | Intellian | V100 Firmware | 1.20 | All | All | All |
| Operating System | Intellian | V100 Firmware | 1.21 | All | All | All |
| Operating System | Intellian | V100 Firmware | 1.24 | All | All | All |
| Hardware | Intellian | V60 | - | All | All | All |
| Hardware | Intellian | V60 | - | All | All | All |
| Operating System | Intellian | V60 Firmware | 1.15 | All | All | All |
| Operating System | Intellian | V60 Firmware | 1.25 | All | All | All |
| Operating System | Intellian | V60 Firmware | 1.15 | All | All | All |
| Operating System | Intellian | V60 Firmware | 1.25 | All | All | All |
| Application | Mitel | Micollab | 6.0 | All | All | All |
| Application | Mitel | Micollab | 7.0 | All | All | All |
| Application | Mitel | Micollab | 7.1 | All | All | All |
| Application | Mitel | Micollab | 7.2 | All | All | All |
| Application | Mitel | Micollab | 7.3 | All | All | All |
| Application | Mitel | Micollab | 7.3.0.104 | All | All | All |
| Application | Mitel | Micollab | 6.0 | All | All | All |
| Application | Mitel | Micollab | 7.0 | All | All | All |
| Application | Mitel | Micollab | 7.1 | All | All | All |
| Application | Mitel | Micollab | 7.2 | All | All | All |
| Application | Mitel | Micollab | 7.3 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Mitel | Micollab | 7.3.0.104 | All | All | All |
| Application | Mitel | Mivoice | 1.1.2.5 | All | All | All |
| Application | Mitel | Mivoice | 1.1.3.3 | All | All | All |
| Application | Mitel | Mivoice | 1.2.0.11 | All | All | All |
| Application | Mitel | Mivoice | 1.3.2.2 | All | All | All |
| Application | Mitel | Mivoice | 1.4.0.102 | All | All | All |
| Application | Mitel | Mivoice | 1.1.2.5 | All | All | All |
| Application | Mitel | Mivoice | 1.1.3.3 | All | All | All |
| Application | Mitel | Mivoice | 1.2.0.11 | All | All | All |
| Application | Mitel | Mivoice | 1.3.2.2 | All | All | All |
| Application | Mitel | Mivoice | 1.4.0.102 | All | All | All |
| Application | Openssl | Openssl | All | All | All | All |
| Application | Openssl | Openssl | All | All | All | All |
| Operating System | Opensuse | Opensuse | 12.3 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |
| Operating System | Opensuse | Opensuse | 12.3 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Application | Redhat | Gluster Storage | 2.1 | All | All | All |
| Application | Redhat | Gluster Storage | 2.1 | All | All | All |
| Application | Redhat | Storage | 2.1 | All | All | All |
| Application | Redhat | Storage | 2.1 | All | All | All |
| Application | Redhat | Virtualization | 6.0 | All | All | All |
| Application | Redhat | Virtualization | 6.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Hardware | Ricon | S9922l | 1.0 | All | All | All |
| Operating System | Ricon | S9922l Firmware | 16.10.3\(3794\) | All | All | All |
| Hardware | Siemens | Application Processing Engine | - | All | All | All |
| Hardware | Siemens | Application Processing Engine | - | All | All | All |
| Operating System | Siemens | Application Processing Engine Firmware | 2.0 | All | All | All |
| Operating System | Siemens | Application Processing Engine Firmware | 2.0 | All | All | All |
| Hardware | Siemens | Cp 1543-1 | - | All | All | All |
| Hardware | Siemens | Cp 1543-1 | - | All | All | All |
| Operating System | Siemens | Cp 1543-1 Firmware | 1.1 | All | All | All |
| Operating System | Siemens | Cp 1543-1 Firmware | 1.1 | All | All | All |
| Application | Siemens | Elan-8.2 | All | All | All | All |
| Application | Siemens | Elan-8.2 | All | All | All | All |
| Hardware | Siemens | Simatic S7-1500 | - | All | All | All |
| Hardware | Siemens | Simatic S7-1500 | - | All | All | All |
| Hardware | Siemens | Simatic S7-1500t | - | All | All | All |
| Hardware | Siemens | Simatic S7-1500t | - | All | All | All |
| Operating System | Siemens | Simatic S7-1500t Firmware | 1.5 | All | All | All |
| Operating System | Siemens | Simatic S7-1500t Firmware | 1.5 | All | All | All |
| Operating System | Siemens | Simatic S7-1500 Firmware | 1.5 | All | All | All |
| Operating System | Siemens | Simatic S7-1500 Firmware | 1.5 | All | All | All |
| Application | Siemens | Wincc Open Architecture | 3.12 | All | All | All |
| Application | Siemens | Wincc Open Architecture | 3.12 | All | All | All |

## References

| Reference |
|---|
| '[security bulletin] HPSBMU03033 rev.1 - HP Insight Control Software Components running OpenSSL, Remo' - MARC |
| www.innominate.com/data/downloads/manuals/mdm_1.5.2.1_Release_Notes.pdf |
| '[security bulletin] HPSBHF03293 rev.1 - HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and' - MARC |
| '[security bulletin] HPSBMU03019 rev.1 - HP Software UCMDB Browser and Configuration Manager running ' - MARC |
| Viestintävirasto - Information security |
| '[security bulletin] HPSBMU03023 rev.1 - HP BladeSystem c-Class Virtual Connect Support Utility (VCSU' - MARC |
| Mageia Advisory: MGASA-2014-0165 - Updated openssl package fix two security vulnerabilities |
| '[security bulletin] HPSBMU03030 rev.1 - HP Service Pack for ProLiant (SPP) Bundled Software running ' - MARC |
| Chef Server Heartbleed (CVE-2014-0160) Releases \| Chef Blog |
| [SECURITY] Fedora 19 Update: openssl-1.0.1e-37.fc19.1 |
| openSUSE-SU-2014:0560-1: moderate: update for openssl |

Apache Mail Archives

Red Hat Customer Portal

Issue 85 - mod-spdy - CVE-2014-0160 fix needed - Apache SPDY module - Google Project Hosting

Red Hat Customer Portal

OpenSSL TLS Heartbeat Extension - Memory Disclosure

Security Advisory SA59347 - Innominate mGuard Device Manager OpenSSL Multiple Vulnerabilities - Secunia

Vulnerabilities resolved in TRITON APX Version 8.0

WebEx Meetings Server OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Information - SecurityTrac

'[security bulletin] HPSBMU03024 rev.1 - HP Insight Control Server Deployment on Linux and Windows ru' - MARC

'[security bulletin] HPSBPI03014 rev.1 - HP LaserJet Pro MFP Printers, HP Color LaserJet Pro MFP Prin' - MARC

Full Disclosure: heartbleed OpenSSL bug CVE-2014-0160

OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Information - SecurityTracker

'[security bulletin] HPSBMU03022 rev.1 - HP Systems Insight Manager (SIM) Bundled Software running Op' - MARC

Cisco Security Manager OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Information - SecurityTrack

'[security bulletin] HPSBMU03037 rev.2 - HP Multimedia Service Environment (MSE), (HP Network Interac' - MARC

VMSA-2014-0012 | United States

OpenSSL ‘heartbleed’ bug live blog | Fox-IT International blog

'[security bulletin] HPSBMU03025 rev.1 - HP Diagnostics running OpenSSL, Remote Disclosure of Informa' - MARC

SOL15159 - OpenSSL vulnerability CVE-2014-0160

Security Advisory SA57721 - Debian update for openssl - Secunia

BlackBerry Link OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Information - SecurityTracker

'[security bulletin] HPSBMU03028 rev.1 - HP Matrix Operating Environment and CloudSystem Matrix Softw' - MARC

Heartbleed Bug

About Secunia Research | Flexera

'[security bulletin] HPSBMU03032 rev.1 - HP Virtual Connect Firmware Smart Components Installer Softw' - MARC

'[security bulletin] HPSBMU03012 rev.1 - HP Insight Management VCEM Web Client SDK (VCEMSDK) running ' - MARC

'[security bulletin] HPSBGN03010 rev.1 - HP Software Server Automation, "HeartBleed" OpenSSL Vulnerab' - MARC

Security Advisory SA59139 - Schneider Electric Network Shutdown Module (NSM) OpenSSL Heartbeat Two Vulnerabilities - Secunia

IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.3.0.1 Interim Fix 29 README Tivoli Composite Appl

git.openssl.org Git - openssl.git/commit

'[security bulletin] HPSBST03015 rev.1 - HP 3PAR OS running OpenSSL, Remote Disclosure of Information' - MARC

Enterprise Chef 11.1.3 Release | Chef Blog

About Secunia Research | Flexera

Full Disclosure: MRI Rubies may contain statically linked, vulnerable OpenSSL

F5 - Signon

'[security bulletin] HPSBHF03126 rev.1 - HP TippingPoint NGFW running OpenSSL, Remote Disclosure of I' - MARC

[security bulletin] HPSBHF03136 rev.1 - HP TippingPoint NGFW running OpenSSL, Remote Disclosure of I - MARC

'[security bulletin] HPSBMU03009 rev.2 - HP CloudSystem Foundation and Enterprise Software v8.0 runni' - MARC

Splunk OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Information - SecurityTracker

'[security bulletin] HPSBMU03062 rev.1 - HP Insight Control server deployment on Linux and Windows ru' - MARC

'[security bulletin] HPSBPI03031 rev.1 - HP Officejet Pro X Printers, Certain Officejet Pro Printers,' - MARC

'[security bulletin] HPSBST03004 rev.1 - HP IBRIX X9320 Storage running OpenSSL, Remote Disclosure of' - MARC

Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities

Release Notes

git.openssl.org Git - openssl.git/commit

Security Advisories Relating to Symantec Products - Symantec Messaging Gateway 10.6.x ACE Library Static Link to Vulnerable SSL Version

cert-portal.siemens.com/productcert/pdf/ssa-635659.pdf

KB35882-BlackBerry response to OpenSSL “Heartbleed” vulnerability

FileZilla - The free FTP solution

IBM Security Bulletin: IBM DS8870 Release 7.2 is affected by an additional vulnerability in OpenSSL (CVE-2014-0160) - United States

Debian -- Security Information -- DSA-2896-1 openssl

'[security bulletin] HPSBHF03021 rev.1 - HP Thin Client with ThinPro OS or Smart Zero Core Services, ' - MARC

Vulnerability Report - "Heartbleed" security vulnerability found in certain versions of SAN Datamover used in Unisys MCP Platforms

'[security bulletin] HPSBST03016 rev.1 - HP P2000 G3 MSA Array Systems, HP MSA 2040 Storage, and HP M' - MARC

Bug 1084875 – CVE-2014-0160 openssl: information disclosure in handling of TLS heartbeat extension packets

Mitel Product Security Advisory 17-0008

About Secunia Research | Flexera

OpenSSL 1.0.1f TLS Heartbeat Extension - Memory Disclosure (Multiple SSL/TLS versions)

Support / Security / Advisories / / MDVSA-2015:062 | Mandriva

OpenSSL Heartbleed Vulnerability CVE-2014-0160

'[security bulletin] HPSBMU02999 rev.1 - HP Software Autonomy WorkSite Server (On-Premises Software),' - MARC

OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products

RICON Industrial Cellular Router Heartbleed Attack - Yunus Şahin - Medium

Apache Mail Archives

OpenSSL bug CVE-2014-0160 | The Tor Blog

'[security bulletin] HPSBMU03029 rev.1 - HP Insight Control Server Migration running OpenSSL, Remote ' - MARC

Citrix Security Advisory for CVE-2014-0160, aka the Heartbleed vulnerability

IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.4 Interim Fix 13 README Tivoli Composite Applicati

[SECURITY] Fedora 20 Update: openssl-1.0.1e-37.fc20.1

Cisco Unified Communications Manager OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Informatio

Pony Mail!

'[security bulletin] HPSBMU03017 rev.1 - HP Software Connect-IT running OpenSSL, Remote Disclosure of' - MARC

'[security bulletin] HPSBMU02997 rev.1 - HP Smart Update Manager (SUM) running OpenSSL, Remote Disclo' - MARC

Vulnerability Report - OpenSSL "Heartbleed" vulnerability on OS 2200 QProcessor

OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160) | US-CERT

'[security bulletin] HPSBST03027 rev.1 - HP StoreVirtual 4000 Storage and HP P4000 G2 Storage using H' - MARC

'[security bulletin] HPSBMU03040 rev.1 - HP LoadRunner & HP Performance Center, running OpenSSL, Remo' - MARC

[syslog-ng-announce] syslog-ng Premium Edition 5 LTS (5.0.4a) has been released

'[security bulletin] HPSBGN03011 rev.1 - HP IceWall MCRP running OpenSSL on Red Hat Enterprise Linux ' - MARC

Full Disclosure: Re: heartbleed OpenSSL bug CVE-2014-0160

About Secunia Research | Flexera

Full Disclosure: Re: heartbleed OpenSSL bug CVE-2014-0160

Check your system rubies for vulnerable OpenSSL (CVE-2014-0160 "Heartbleed")

[security-announce] openSUSE-SU-2014:0492-1: important: update for opens

Oracle Critical Patch Update - July 2014

Full Disclosure: Re: heartbleed OpenSSL bug CVE-2014-0160

About Secunia Research | Flexera

'[security bulletin] HPSBMU03018 rev.1 - HP Software Asset Manager running OpenSSL, Remote Disclosure' - MARC

Pony Mail!

Skull Army: #Heartbleed; The hearts continue to bleed...

Red Hat Customer Portal

'[security bulletin] HPSBGN03008 rev.1 - HP Software Service Manager, "HeartBleed" OpenSSL Vulnerabil' - MARC

Kerio Control small business firewall

'[security bulletin] HPSBST03001 rev.1 - HP XP P9500 Disk Array running OpenSSL, Remote Disclosure of' - MARC

Pony Mail!

Cisco Mobility Services Engine OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Information - Securi

Cisco IOS XE OpenSSL TLS Heartbeat Buffer Overread Lets Remote Users Obtain Potentially Sensitive Information - SecurityTracker

Apache Mail Archives

SecurityFocus

'[security bulletin] HPSBMU02995 rev.1 - HP Software HP Service Manager, Asset Manager, UCMDB Browser' - MARC

Security Advisory SA59243 - IBM DS8870 OpenSSL TLS/DTLS Heartbeat Two Information Disclosure Vulnerabilities - Secunia

'[security bulletin] HPSBMU02998 rev.1 - HP System Management Homepage (SMH) running OpenSSL on Linux' - MARC

'[security bulletin] HPSBMU03044 rev.1 - HP Business Process Monitor, running OpenSSL, Remote Disclos' - MARC

USN-2165-1: OpenSSL vulnerabilities | Ubuntu

Please wait...

[SECURITY] Fedora 20 Update: openssl-1.0.1e-39.fc20

'[security bulletin] HPSBMU03013 rev.1 - WMI Mapper for HP Systems Insight Manager running OpenSSL, R' - MARC

| |
|---|
| Red Hat Customer Portal |
| '[security bulletin] HPSBMU03020 rev.1 - HP Version Control Agent (VCA) and Version Control Repositor' - MARC |
| OpenSSL TLS 'heartbeat' Extension Multiple Information Disclosure Vulnerabilities |
| Enterprise Chef 1.4.9 Release \| Chef Blog |
| HP Support document - HP Support Center |
| Chef Server 11.0.12 Release \| Chef Blog |
| www.openssl.org/news/secadv_20140407.txt |
| Pony Mail! |
| Apache Mail Archives |
| News - Product Security - Security advisories - 2014 - fsc-2014-1 \| F-Secure |
| Splunk 6.0.3 addresses two vulnerabilities - April 10, 2014 \| Splunk |
| [security-announce] SUSE Security Announcement: openssl "HeartBleed" att |
| IBM Security Bulletin: IBM Endpoint Manager 9.1.1065 – OpenSSL Vulnerability Update (CVE-2014-0160) - United States |
| Schneider Electric |
| Vulnerability Note VU#720951 - OpenSSL TLS heartbeat extension read overflow discloses sensitive information |
| '[security bulletin] HPSBMU02994 rev.1 - HP BladeSystem c-Class Onboard Administrator (OA) running Op' - MARC |
| CVE Program record |
| NVD vulnerability detail |
| CISA Known Exploited Vulnerabilities catalog |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

390226 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

390284 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

690308 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (5631ae98-be9e-11e3-b5e3-c80aa9043978)