Westcon CVE-2014-0160 advisory

Table of Contents

Inside CVE 2014-0160

Common Vulnerabilities and Exposure report (CVE) 2014 – 0160 was released for a bug in OpenSSL.
This vulnerability is also known as “The Heartbleed Bug”.

Westcon CVE-2014-0160 advisory

Description:

The implementation of TLS/DTLS in versions 1.0.1a through 1.0.1f , and 1.0.2 through 1.0.2-beta1 of OpenSSL doesn't properly handle Heartbeat Extension packets.

There is a missing bounds check in the handling of the TLS/DTLS Heartbeat extension. (Hence the name "Heartbleed" bug).

A specially crafted TLS Hello packet that includes the Heartbeat extension codes can be used to repeatedly retrieve chunks of up to 64 kilobytes of memory from the vulnerable server.
With this attackers can read the entire contents of the RAM memory of the vulnerable server revealing protected data.

Normally the response packet of a TLS Hello contains 3 bytes of information. Due to the fact that there are no bounds checks in the function(s) that handle the Heartbeat extension it's possible to tell the server to send more data, the attacker can even specifically select from which memory address the chunk of data has to be read.

What's revealed?

This data is unencrypted thereby revealing important, private, information.
This includes:

- Primary secret keys (**Private SSL Certificate key!**)
- Usernames
- Passwords
- Your private information that was supposed to be encrypted

Impact:

OpenSSL is used by more than 2/3rd of all webservers in the world.

Many products of our vendors are also vulnerable; this document contains their security advisories.
Please note that not all ramifications of this vulnerability are clear yet.

IPS/IDS & AV vendors do have detection patterns available update and upgrade your products immediately.

This bug allows attackers to decrypt SSL encrypted communication and impersonate service providers.

Discovery:

The vulnerability that has existed since 2011 was revealed to the OpenSSL community by Neel Mehta of Google security.
A fix was developed by Adam Langley (Chromium.Org) and Bodo Moeller (ACM.Org).

A fix has been implemented in OpenSSL 1.0.1g. Version 1.0.2 will be fixed in 1.0.2-beta2.
Versions older than 1.0.1 are not vulnerable.

Tests:

From github you can download a Perl5 script to test this vulnerability.
https://github.com/noxxi/p5-scripts/blob/master/check-ssl-heartbleed.pl

Duplicate CVE:

CVE 2014-0346 is in fact a duplicate of CVE 2014-0160 and should not be used. The duplication was caused due to coincidentally 2 different people found the same bug, approximately at the same time, independently from eachother.

Sources:

US-CERT
OpenSSL
Thawte
Mitre

Blue Coat

Security Advisories

April 9, 2014 – OpenSSL heartbeat information disclosure (CVE-2014-0160)

Westcon CVE-2014-0160 advisory

Back to all Security Advisories Printer Friendly Rate this Page

Security Advisories ID:	SA79
Version:	7.0
Status:	Published
Published date:	04/08/2014
Updated:	04/09/2014
Applies To:	Director, IntelligenceCenter, PacketShaper, ProxyAV, ProxySG, Reporter, PolicyCenter, CacheFlow, DLP, Management Center

Advisory Status

Interim

Advisory Severity

Medium - CVSS v2 base score: 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVE Number

CVE-2014-0160 – CVSS base score: 9.4 (AV:N/AC:L/Au:N/C:C/I:C/A:N)

Summary

Blue Coat products using affected versions of OpenSSL 1.0.1 that support TLS/DTLS heartbeats are vulnerable to a buffer over-read that discloses information kept in process memory. A remote attacker may exploit this vulnerability to obtain keys, passwords, and other sensitive data kept in memory.

Westcon CVE-2014-0160 advisory

Affected Products

The following products are vulnerable:

Content Analysis System

CAS 1.1.1.1 through 1.1.5.1 (inclusive) are vulnerable.

Malware Analysis Appliance

MAA 1.1.1 is vulnerable.

ProxyAV

ProxyAV 3.5.1.1 through 3.5.1.6 (inclusive) are vulnerable. Previous versions do not use versions of OpenSSL that are affected and are therefore not vulnerable.

ProxySG

ProxySG from 6.5.1.1 through 6.5.3.5 (inclusive) are vulnerable. Reverse and forward proxy are vulnerable, as are management interfaces. Previous versions do not use versions of OpenSSL that are affected and are therefore not vulnerable.

SSL Visibility

SSL Visibility version 3.7.0 is vulnerable. Previous versions do not use versions of OpenSSL that are affected and are therefore not vulnerable. Only TLS connections to the management plane are vulnerable; TLS connections to the data plane do not use OpenSSL and are therefore not affected.

Westcon CVE-2014-0160 advisory

The following products are not vulnerable:

CacheFlow

Director

DLP

IntelligenceCenter

PacketShaper

PacketShaper S-series

PolicyCenter

Reporter

Security Analytics Platform

X-Series

Details

CVE-2014-0160 (VU#720951) is a buffer over-read flaw in the OpenSSL implementation of the TLS/DTLS heartbeat functionality. The vulnerability is addressed in OpenSSL 1.0.1g. OpenSSL 1.0.1 through 1.0.1f are vulnerable. Vulnerable versions do not handle the heartbeat extension packets properly and will return additional information from the server's adjacent process memory to the requester.

Blue Coat products using a vulnerable version of OpenSSL with the heartbeat option enabled are vulnerable. This vulnerability only applies to products acting as a server in the TLS session.

An attacker may exploit this flaw to download up to 64 kB of private memory from a server. The attacker cannot specify the location of the memory to read. The exploit can be employed repeatedly to obtain as much information as desired. There is no way to detect that an attacker has exploited this vulnerability or to know what portions of memory may be provided.

Memory may contain private keys, symmetric keys, user names, passwords, data used by the service, and data from TLS connections. An attacker could use this information to become a man-in-the-middle for other connections and decrypt traffic previously intercepted. An attacker may also use the passwords to impersonate a user or a client.

Westcon CVE-2014-0160 advisory

Workarounds

Until patches are made available, the following workarounds may be applied.

Downgrade to a previous version that is not vulnerable. Select the latest patch release available for ProxyAV 3.4, ProxySG 6.4, and SSL Visibility 3.6.

Restrict access to vulnerable products, especially to administrative functionality.

Patches

After installing a patch, customers are urged to employ recovery procedures including revoking certificates for private keys that may have been compromised, changing passwords that may have been compromised, and notifying users of possible data leakage.

Content Analysis System

CAS 1.1 – a fix is not yet available.

Malware Analysis System

MAA 1.1 – a fix is not yet available.

ProxyAV

ProxyAV 3.5 – a fix is not yet available.

ProxySG

ProxySG 6.5.3 – a fix is available in patch release 6.5.3.6 and later.

ProxySG 6.5.2 – a fix is not yet available.

SSL Visibility

SSL Visibility 3.7 – a workaround fix is available in patch 3.7.0-69 to disable heartbeat.

Fixes are available to customers with a valid Blue Touch Online login. Please visit the Downloads section of BTO at https://bto.bluecoat.com/flexera.

Westcon CVE-2014-0160 advisory

References

CVE-2014-0160 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160

Vulnerability Note VU#720951 - http://www.kb.cert.org/vuls/id/720951

OpenSSL advisory - http://www.openssl.org/news/secadv_20140407.txt

Heartbleed website - http://heartbleed.com/

Advisory History

2014-04-09 Added PacketShaper S500 as not vulnerable.

2014-04-09 Further refinement on exact versions of ProxyAV that are vulnerable.

2014-04-09 Further refinement on exact versions of CAS and MAA that are vulnerable.

2014-04-09 Minor clarification on restricting access as a workaround.

2014-04-09 Minor update to specify exact version of SSL Visibility that is vulnerable.

2014-04-09 Initial public release

Westcon CVE-2014-0160 advisory

Checkpoint

Check Point response to OpenSSL vulnerability (CVE-2014-0160)

Solution ID: sk100173
Severity: Low
Product: Security Gateway, Security Management, Multi-Domain Management / Provider-1, Data Center Security Appliances, Endpoint Security Server, Endpoint Connect, SSL Network Extender
Version: All
OS: Gaia, Gaia Embedded, SecurePlatform 2.6, SecurePlatform Embedded, IPSO 6.2
Platform / Model: All
Date Created: 08-apr-2014

Symptoms

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not handle properly Transport Layer Security protocols (TLS/DTLS) Heartbeat Extension packets. As a result, remote attackers could obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys.

Solution

Checking the OpenSSL version

Show / Hide instructions
To check the current version of OpenSSL, run this command:

On Gaia OS

```
[Expert@HostName]# rpm -qa | grep openssl
```

Example output:

```
openssl-0.9.8b-8.3cp738000011
```

On SecurePlatform OS

```
[Expert@HostName]# rpm -qa | grep openssl
```

Example output:

```
openssl-libcrypto-0.9.7a-36cp
```

On IPSO OS 6

```
# openssl version
```

Please find the most recent version of this article online in the Checkpoint knowledgebase:
http://supportcontent.checkpoint.com/solutions?id=sk100173

Westcon CVE-2014-0160 advisory

Infoblox

Summary:
1. Infoblox DDI and NetMRI products are not affected by the “Heartbleed” defect announced by the OpenSSL project. We encourage users of the products to check back periodically for any updates.

2. Infoblox Customer Support Portal has been patched to address the “Heartbleed” vulnerability – although we have not identified a breach of our systems, customers are strongly encouraged to reset their support portal passwords.

Dear Infoblox Customer,

On April 7, 2014, it was announced that certain versions of OpenSSL had a severe memory handling defect. This defect, informally known as “Heartbleed,” could be exploited by attackers to read the memory of systems using vulnerable versions of the OpenSSL open source library.

No Impact on Infoblox Products
Based on the Heartbleed CVE issued by the OpenSSL project (CVE-2014-0160), Infoblox has determined that the products listed below are not affected by the OpenSSL defect. No action to remediate the OpenSSL defect is required for the Infoblox products at this time.

Infoblox products:

- All Infoblox DDI products running NIOS
- All Infoblox Network Automation products including NetMRI, Switch Port Manager, Automation Change Manager, Security Device Controller

For Infoblox Support Portal Users:
For customers accessing Infoblox support via the Infoblox Support Portal, the appropriate systems have been patched and updated to address the defect.

As a precaution, we strongly encourage that you change your support portal password (once you login, please find the “Change Your Password” link under “Account Settings”)

If you have additional questions or concerns, please don’t hesitate to contact Infoblox Support.

For More Detail Please See Reference Material

- Infoblox Knowledge Base
- Department of Homeland Security National Vulnerability Database
- Common Vulnerabilities and Exposures Website (CVE) Article

Westcon CVE-2014-0160 advisory

F-Secure

Heartbleed OpenSSL vulnerability guidance

The HeartBleed OpenSSL vulnerability affects services using the affected versions of OpenSSL. Also some F-Secure services and products are affected by this.
While our development and hosting teams have been working to patch the vulnerable services, to renew possibly affected certificates and changing credentials, we would advise all customers to change their passwords, both in services used at home and at the office. For a list of affected online services, please see the article "The Heartbleed Hit List: The Passwords You Need to Change Right Now".
F-Secure will release a centralized security advisory, which we will keep updating with more information as we go.
Please follow the address:
http://www.f-secure.com/en/web/labs_global/security-advisories
to get up-to-date information on the topic.
Some customers can expect further information and advice regarding the services they use and actions they should take.

What is HeartBleed?

HeartBleed is a critical security vulnerability in the OpenSSL library. This library is widely used on the Internet to provide secure connections, and the vulnerability potentially allows an attacker to silently read information from the memory of a server, or a malicious server to read the memory of a client. This means highly confidential information, such as web server private keys and user passwords, could be copied by an attacker. The vulnerability has existed for more than two years before it was discovered and fixed in the library. Read more about HeartBleed and how to secure yourself against it in the blog post "You're going to need to change your passwords — and here's the easiest way to do it"

Westcon CVE-2014-0160 advisory

F5

SOL15159: OpenSSL vulnerability CVE-2014-0160

Security Advisory
Original Publication Date: 04/08/2014
Updated Date: 04/08/2014
Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.(CVE-2014-0160)

Impact

Systems that are vulnerable can be exploited to retrieve information from memory. That information may include the private keys used for TLS/DTLS.
Virtual servers using an SSL profile configured with the default Native SSL ciphers are not vulnerable. Only virtual servers using an SSL profile configured to use ciphers from the Compat SSL stack are vulnerable. In addition, back-end resources are not protected by virtual servers that do not use SSL profiles and pass SSL traffic directly through to the back-end web servers.
The Configuration utility on the management interface is vulnerable.
Clients using the BIG-IP Edge client for Android are not vulnerable to this vulnerability. However, clients using the BIG-IP Edge client for Windows, Mac OS, or Linux are vulnerable if they are used to connect to a compromised FirePass or BIG-IP APM system.

Westcon CVE-2014-0160 advisory

Status

F5 Product Development has assigned ID 456033 (BIG-IP) to this vulnerability.
To determine if your release is known to be vulnerable, the components or features that are affected by the vulnerability, and for information about releases or hotfixes that address the vulnerability, refer to the following table:

Product	Versions known to be vulnerable	Versions known to be not vulnerable	Vulnerable component or feature
BIG-IP LTM	11.5.0 - 11.5.1	11.0.0 - 11.4.1 10.0.0 - 10.2.4	Configuration utility Compat SSL ciphers
BIG-IP AAM	11.5.0 - 11.5.1	11.4.0 - 11.4.1	Configuration utility Compat SSL ciphers
BIG-IP AFM	11.5.0 - 11.5.1	11.3.0 - 11.4.1 None	Configuration utility Compat SSL ciphers
BIG-IP Analytics	11.5.0 - 11.5.1	11.0.0 - 11.4.1 None	Configuration utility Compat SSL ciphers
BIG-IP APM	11.5.0 - 11.5.1	11.0.0 - 11.4.1 10.1.0 - 10.2.4 None	Configuration utility Compat SSL ciphers
BIG-IP ASM	11.5.0 - 11.5.1	11.0.0 - 11.4.1 10.0.0 - 10.2.4 None	Configuration utility Compat SSL ciphers
BIG-IP Edge Gateway	None	11.0.0 - 11.3.0 10.1.0 - 10.2.4	None
BIG-IP GTM	11.5.0 - 11.5.1	11.0.0 - 11.4.1 10.0.0 - 10.2.4 None	Configuration utility Compat SSL ciphers
BIG-IP Link Controller	11.5.0 - 11.5.1	11.0.0 - 11.4.1 10.0.0 - 10.2.4	Configuration utility Compat SSL ciphers
BIG-IP PEM	11.5.0 - 11.5.1	11.3.0 - 11.4.1	Configuration utility Compat SSL ciphers
BIG-IP PSM	11.5.0 - 11.5.1	11.0.0 - 11.4.1 10.0.0 - 10.2.4 None	Configuration utility Compat SSL ciphers
BIG-IP WebAccelerator	None	11.0.0 - 11.3.0 10.0.0 - 10.2.4	None
BIG-IP WOM	None	11.0.0 - 11.3.0 10.0.0 - 10.2.4	None
ARX	None	6.0.0 - 6.4.0	None
Enterprise Manager	None	3.0.0 - 3.1.1 2.1.0 - 2.3.0	None
FirePass	None	7.0.0 6.0.0 - 6.1.0	None
BIG-IQ Cloud	None	4.0.0 - 4.3.0	None
BIG-IQ Device	None	4.2.0 - 4.3.0	None
BIG-IQ Security	None	4.0.0 - 4.3.0	None
BIG-IP Edge Clients for Android	None	2.0.3 - 2.0.4	None
BIG-IP Edge Clients for Apple iOS	2.0.0 - 2.0.1 1.0.5	1.0.0 - 1.0.4	VPN
BIG-IP Edge Clients for Linux	7080 - 7101	6035 - 7071	VPN
BIG-IP Edge Clients for MAC OS X	7080 - 7101	6035 - 7071	VPN
BIG-IP Edge Clients for Windows	7080 - 7101	6035 - 7071	VPN

Westcon CVE-2014-0160 advisory

Recommended action

If the previous table lists a version in the **Versions known to be not vulnerable** column, you can eliminate this vulnerability by upgrading to the listed version. If the table does not list any version in the column, then no upgrade candidate currently exists.
To mitigate this vulnerability, you should consider the following recommendations:
Limit the Configuration utility access to a trusted management network.
Use only Native SSL stack ciphers. Do not use ciphers from the Compat SSL stack. For information about the Native and Compat ciphers, refer to SOL13163: SSL ciphers supported on BIG-IP platforms (11.x).
Back-end resources are not protected by virtual servers that do not use SSL profiles and pass SSL traffic through to the back-end web servers. When possible, you should protect back-end resources by using SSL profiles to terminate SSL at the BIG-IP.
Supplemental Information
http://heartbleed.com/
SOL12463: Overview of F5 Edge products
SOL13757: BIG-IP Edge Client version matrix
SOL9970: Subscribing to email notifications regarding F5 products
SOL9957: Creating a custom RSS feed to view new and updated documents.
SOL4602: Overview of the F5 security vulnerability response policy
SOL4918: Overview of the F5 critical issue hotfix policy
SOL167: Downloading software and firmware from F5
SOL13123: Managing BIG-IP product hotfixes (11.x)
SOL10025: Managing BIG-IP product hotfixes (10.x)
SOL9502: BIG-IP hotfix matrix
SOL10322: FirePass hotfix matrix

Westcon CVE-2014-0160 advisory

Juniper

▼ [JSA10623] Show KB Properties

PRODUCT AFFECTED:

Various products: Please see the list in the problem section

PROBLEM:

The TLS and DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeart Extension packets, which allows remote attackers to obtain sensitive information (such as private keys, username and passwords, or contents of encrypted traffic) from process memory via crafted packets that trigger a buffer over-read. This issue is also known as The Heartbleed Bug.

Status of different OpenSSL versions:
OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
OpenSSL 1.0.1g is NOT vulnerable
OpenSSL 1.0.0 branch is NOT vulnerable
OpenSSL 0.9.8 branch is NOT vulnerable

Vulnerable Products

- **Junos OS 13.3R1**
- **Odyssey client 5.6r5 and later**
- **SSL VPN (IVEOS) 7.4r1 and later, and SSL VPN (IVEOS) 8.0r1 and later (Fixed code is listed in the "Solution" section)**
- **UAC 4.4r1 and later, and UAC 5.0r1 and later (Fixed code is listed in the "Solution" section)**
- **Junos Pulse (Desktop) 5.0r1 and later, and Junos Pulse (Desktop) 4.0r5 and later**
- **Network Connect (windows only) version 7.4R5 to 7.4R9.1 & 8.0R1 to 8.0R3.1. (This client is only impacted when used in FIPS mode.)**
- **Junos Pulse (Mobile) on Android version 4.2R1 and higher.**
- **Junos Pulse (Mobile) on iOS version 4.2R1 and higher. (This client is only impacted when used in FIPS mode.)**

Westcon CVE-2014-0160 advisory

Products Not Vulnerable

- **Junos OS 13.2 and earlier is not vulnerable**
- **Non-FIPS version of Network Connect clients are not vulnerable**
- **SSL VPN (IVEOS) 7.3, 7.2, and 7.1 are not vulnerable**
- **SRX Series is not vulnerable**
- **Junos Space is not vulnerable**
- **NSM is not vulnerable**
- **Pulse 4.0r4 and earlier is not vulnerable**
- **QFabric Director is not vulnerable**
- **CTPView is not vulnerable**
- **vGW/FireFly Host is not vulnerable**
- **Firefly Perimeter is not vulnerable**
- **ScreenOS is not vulnerable**
- **UAC 4.3, 4.2, and 4.1 are not vulnerable**
- **JUNOSe is not vulnerable**
- **Odyssey client 5.6r4 and earlier are not vulnerable**
- **Junos Pulse (Mobile) on iOS (Non-FIPS Mode)**
- **WX-Series is not vulnerable**
- **Junos DDoS Secure is not vulnerable**
- **STRM/JSA is not vulnerable**
- **WebApp Secure is not vulnerable**
- **Media Flow Controller is not vulnerable**
- **SBR Carrier is not vulnerable**
- **SBR Enterprise is not vulnerable**
- **Junos Pulse Mobile Security Suite is not vulnerable**
- **SRC Series is not vulnerable**

Products currently under investigation

- **Stand Alone IDP**
- **ADC**
- **WL-Series (SmartPass)**

Juniper continues to investigate this issue and as new information becomes available this document will be updated.

This issue has been assigned CVE-2014-0160.
SOLUTION:

We are working around the clock to provide fixed versions of code for our affected products.

SSL VPN (IVEOS):
Juniper Networks has released IVEOS 8.0R3.1 and 7.4R9.1. For more information surrounding this issue for this platform please see KB: http://kb.juniper.net/kb29004

UAC:
Juniper Networks will release (ETA April 10th, 2014) UAC 5.0r3.2. For more information surrounding this issue for this platform please see KB: http://kb.juniper.net/kb29007

Junos:
Junos OS 13.3R1.6, 13.3R1.7, and 13.3R1-S1 have been recalled and will be re-released with fixes to resolve this issue.

Westcon CVE-2014-0160 advisory

IDP Signatures:
Juniper has released signatures to detect this issue:

Sigpack 2362 released:
https://signatures.juniper.net/restricted/sigupdates/nsm-updates/updates.xml
https://signatures.juniper.net/restricted/sigupdates/nsm-updates/2362.html

SSL: OpenSSL TLS DTLS Heartbeat Information Disclosure:
http://signatures.juniper.net/documentation/signatures/SSL%3AOPENSSL-TLS-DTLS-HEARTBEAT.html

Note: This advisory will be updated with fixed software versions as they are made available to our customers.

KB16765 - "In which releases are vulnerabilities fixed?" describes which release vulnerabilities are fixed as per our End of Engineering and End of Life support policies.

WORKAROUND:

Junos:

- Since SSL is used for remote network configuration and management applications such as J-Web and SSL Service for JUNOScript (XNM-SSL), viable workarounds for this issue in Junos may include:
  - Disabling J-Web
  - Disable SSL service for JUNOScript and only use Netconf, which makes use of SSH, to make configuration changes
  - Limit access to J-Web and XNM-SSL from only trusted networks

SSL VPN/UAC:

- Other than downgrading to an unaffected release, there are no workarounds for this issue.

RELATED LINKS:

- OpenSSL Security Advisory

CVSS SCORE:
9.4 (AV:N/AC:L/Au:N/C:C/I:C/A:N)

RISK LEVEL:

Critical

RISK ASSESSMENT:

We consider this to be a critical issue. The sensitive information potentially exposed by this issue can be leveraged to further compromise the system. Exploits are known to exist in the wild. Information for how Juniper Networks uses CVSS can be found at KB16446 "Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories."

Westcon CVE-2014-0160 advisory

Skybox

Article Number 000001055
Title Are Skybox products vulnerable to CVE-2014-0160 (Heartbleed Bug)?

Summary

The Skybox View Suite is not vulnerable to the Heartbleed bug.
Skybox Appliances are not vulnerable to the Heartbleed bug.
Skybox Virtual Appliances are not vulnerable to the Heartbleed bug.

Background:

The Heartbleed bug is a flaw in OpenSSL's implementation of the TLS/DTLS (transport layer security protocols) heartbeat extension (RFC6520). When it is exploited it leads to the leak of memory contents from the server to the client and from the client to the server.
This is a uniquely severe vulnerability, as it exists on a wide range of products and servers, and allows a potential attacker to gain access to any portion of the server's memory.
In particular, this vulnerability allows access to the private encryption keys used by the server, which would allow the potential attacker to decrypt any data sent to/from the server, that is encrypted using the server's key.

Vulnerable OpenSSL Versions:

OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
OpenSSL 1.0.1g is NOT vulnerable
OpenSSL 1.0.0 branch is NOT vulnerable
OpenSSL 0.9.8 branch is NOT vulnerable

Bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

Skybox Products:

The Skybox View software suite uses JSSE (the Java implemention of SSL), and is therefor NOT vulnerable to the Heartbleed bug.
Skybox Appliances use the OpenSSL library version 1.0.0. They are NOT vulnerable to the Heartbleed bug.
Skybox Virtual Appliances use the OpenSSL library version 1.0.0. They are NOT vulnerable to the Heartbleed bug.
Note that it is possible to manually update the OpenSSL library on Skybox Appliances and Virtual Appliances. It is important that customers confirm their OpenSSL version is still at 1.0.0
To do this, customers can issue the following command on their Appliance or Virtual Appliance:
rpm -q openssl

Customer-managed servers:
Customers who installed Skybox View products on their own servers might be vulnerable to the Heartbleed bug, if their servers run one of the vulnerable OpenSSL versions mentioned above. Customers are advised to update their OpenSSL library as soon as possible.

Summary:
The Skybox View software Suite and Skybox Appliances are NOT vulnerable to the Heartbleed bug. Customers are advised to check the version of their OpenSSL libraries if they are running Skybox products on their own servers (not Skybox Appliances).

Additional Information:
For more information about the Heartbleed bug, please see: http://heartbleed.com/.
For additional information and technical support resources, please contact Skybox Security Support.

Westcon CVE-2014-0160 advisory

Sonicwall

Dell SonicWALL Notice Concerning CVE-2014-0160 OpenSSL Large Heartbeat Response Vulnerability

Researchers have found a critical defect in versions 1.0.1 and 1.0.2-beta of OpenSSL, the cryptographic software library. For information on the vulnerability known as the "Heartbleed bug," see CVE-2014-0160 on the NIST website and heartbleed.com.

Dell SonicWALL Firewalls and Email Security Are Not Affected
Dell SonicWALL firewalls (TZ, NSA, E-Class NSA, SuperMassive) and Email Security are NOT affected by the vulnerability.

Additionally, firewalls with an active Intrusion Prevention Service have, as of April 8th, 2014, signatures to protect vulnerable servers against the vulnerability including Secure Remote Access (SRA) products sitting behind the firewalls.

Dell SonicWALL SRA Specific Firmware Versions Affected

SMB Secure Remote Access

SMB SRA Server Side Firmware
7.0.0.10-26sv and all previous 7.0 versions 7.5.0.3-19sv and all previous 7.5 versions

Impact
Versions above are affected and should be patched immediately.

Recommended Action
Upgrade 7.5 to 7.5.0.4-21sv
Upgrade 7.0 to 7.0.0.11-27sv

E-Class Secure Remote Access (Aventail)
E-Class SRA Server Software

Software version 10.6.4
Software versions 10.7.0 and 10.7.1

Impact
Versions above are affected and should be patched immediately.

Recommended Action
Apply Hotfix 10.6.4-345
Apply Hotfix 10.7.0-582
Apply Hotfix 10.7.1-271

Management and Reporting

Global Management System (GMS) and Analyzer
GMS and Analyzer 7.2 on a Windows platform only

Impact
Version above is affected and should be patched immediately.

Recommended Action
Apply Hotfix 144490 to GMS 7.2 Windows and Analyzer 7.2 Windows systems using the procedure in the hotfix Release Note posted on MySonicWALL.com.

Additional Information

Due to the impact of the OpenSSL vulnerability, products with affected versions can expose user passwords and private keys. Customers may consider resetting passwords and changing keys after patching.

Platform Hotfix for Firmware Version 10.6.4 could be downloaded here**.**
Platform Hotfix for Firmware Version 10.7.0 could be downloaded here **.**
Platform Hotfix for Firmware Version 10.7.1 could be downloaded here**.**

Westcon CVE-2014-0160 advisory

Trend Micro

http://esupport.trendmicro.com/solution/en-US/1103084.aspx

Problem Description

Trend Micro received a vulnerability claim related to the recently published CVE-2014-0160 that could potentially affect its products.

Below is the technical description of the claim:
"The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug."

Solution

Trend Micro has investigated the vulnerability status of the following products. Additional updates and solutions will be posted below as they become available.

Product	Version	Impact Level	Comments/Fix Info
Interscan Web Security Virtual Appliance	All	Not Affected	
ServerProtect for Linux	All	Not Affected	
OfficeScan	All	Not Affected	
Network VirusWall Enforcer	All	Not Affected	
Control Manager	All	Not Affected	
Deep Security	All	Not Affected	
InterScan Messaging Security Virtual Appliance	All	Not Affected	

Westcon CVE-2014-0160 advisory

Tripwire

Tripwire has released a document stating that their websites were vulnerable.
It’s a very interesting read with lots of in depth information, they are fully aware of the ramifications of this bug.

http://www.tripwire.com/state-of-security/security-data-protection/heartbleed-should-give-you-cardiac-arrest/

Westcon CVE-2014-0160 advisory

Vasco

With this communication, we want to inform you about the OpenSSL vulnerability in relation to the VASCO Products

Summary.

Multiple VASCO products incorporate a version of the OpenSSL library affected by a vulnerability that could allow an unauthenticated, remote adversary to retrieve portions of 64 kilobytes from the memory of the VASCO client or server product. This vulnerability is referred to as the Heartbleed bug.

The vulnerability is due to a missing bounds check in the handling of the Transport Layer Security (TLS) heartbeat extension, as specified in RFC 6520. An adversary could exploit this vulnerability by implementing a malicious TLS client, if trying to exploit the vulnerability on an affected server, or a malicious TLS server, if trying to exploit the vulnerability on an affected client. An exploit could send a specially crafted heartbeat packet to the connected client or server. An exploit could allow the adversary to disclose 64 kilobytes of memory from a connected client or server for every heartbeat packet sent. The disclosed portions of memory could contain sensitive data such as private keys, passwords or any data that is exchanged over TLS.
This vulnerability is referred to using the Common Vulnerabilities and Exposures ID CVE-2014-0160.

Affected products.

The following VASCO products are affected by the Heartbleed bug:
Personal aXsGUARD 2.0.0
IDENTIKEY Authentication Server 3.5 and Patch 3.5.1
IDENTIKEY Appliance 3.5.7.0, 3.5.7.1 and 3.5.7.2
IDENTIKEY Virtual Appliance 3.5.7.0, 3.5.7.1 and 3.5.7.2
IDENTIKEY Federation Server 1.3 and 1.4
MYDIGIPASS.COM
DIGIPASS Authentication for Windows Logon 1.2.0
LDAP Synchronization Tool 1.3.0
DIGIPASS Authentication for IIS 3.5.0, DIGIPASS Authentication for Citrix Web Interface 3.6.0, DIGIPASS Authentication for Outlook Web Access 3.5.0, DIGIPASS Authentication for Remote desktop Web Access 3.5.0, DIGIPASS Authentication for SBR 3.5.
The aXsGUARD GateKeeper appliances and other VASCO products are not affected by this bug.

Impact .

The impact of this vulnerability on VASCO products varies depending on the affected product. Successful exploitation of the vulnerability may cause portions of memory from a client or server to be disclosed. The disclosed portions of memory could include sensitive information such as private keys and application-specific data, such as passwords.

Fixed product releases.

VASCO has updated its MYDIGIPASS.COM authentication service on April 9 2014.
VASCO has released patches for following products:
IDENTIKEY Federation Server 1.4.1, released on April 10th 2014
IDENTIKEY Federation Server 1.3.1, released on April 11th 2014
IDENTIKEY Authentication Server 3.5.2, released on April 18th 2014
IDENTIKEY Appliance hotfix + IDENTIKEY Appliance 3.5.7.3, released on April 18th 2014
IDENTIKEY Virtual Appliance hotfix + IDENTIKEY Virtual Appliance 3.5.7.3, released on April 18th 2014
VASCO will release following patches:
Personal aXsGUARD 2.1.0 : release planned for April 25th
Patch for DIGIPASS Authentication for Windows Logon: Release planned in the near future
Patch for LDAP Sync tool: Release planned in the near future
Patch for IIS filters (Citrix, OWA, RDWeb) and DIGIPASS Authentication for SBR: Release planned in the near future
Updates of released patches related to the Heartbleed bug will be published on the VASCO Heartbleed support webpage:

http://www.vasco.com/support/incident-response/security/heartbleed.aspx

Westcon CVE-2014-0160 advisory

Obtaining product releases with fixes.

For IDENTIKEY Federation Server, please contact support@vasco.com
For IDENTIKEY Authentication Server, the patch is available from MyMaintenance
For IDENTIKEY Appliance and IDENTIKEY Virtual appliance, the patch can be installed as an online upgrade by connecting to the VASCO Service Center. Or the offline upgrade package is available from MyMaintenance
For Personal aXsGUARD, the patch will be pushed to the devices automatically from the VASCO Service Center.

Additional recommendations.

Customers with affected products should take following three steps to mitigate the vulnerability:
Step 1: upgrade all affected products using the fixed product releases provided by VASCO
Step 2: revoke SSL/TLS private keys and issue new key pairs and certificates
Due to the bug, it cannot be excluded that SSL/TLS private keys are compromised. Therefore customers should revoke their existing key pairs and certificates and issue new ones.
Step 3: update sensitive data exchanged using SSL/TLS
Customers should assess whether sensitive data (e.g. user passwords, credit card details) exchanged over SSL/TLS might have been compromised. This assessment is specific to the customer. If sensitive data is affected, customers should consider updating this data as well.

References.

http://heartbleed.com
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
http://www.vasco.com/support/support/security/HeartBleed.aspx
Addressing the Heartbleed OpenSSL Bug in Financial Institutions
Addressing the Heartbleed OpenSSL Bug on MYDIGIPASS.COM

Westcon CVE-2014-0160 advisory

Xirrus

Pending