OpenSSL Vulnerability CVS-2014-0160 *(Heartbleed)*

Topic 50519 | Websense Solutions | Published 09-April-2014 | Update #1 for 5-May-2014

Applies To:	Websense security products from version 7.x.x through 7.8.2

Websense software corrections for the OpenSSL Vulnerability CVE-2014-0160 are now posted for customer use. See *Complete Product Tables*, page 2 for instructions.

See this article for an essential added step for installing the TRITON Infrastructure hotfix.

All hotfixes are posted to MyWebsense and (where appropriate) to Appliance download servers.

- All appliances need to be patched, for the affected versions.
- All Web Security Servers need to be patched, for the affected versions.

  *After you install this Hotfix on the Windows Web Security management server, you MUST delete 6 tomcat files:

  Navigate to the Websense installation folder and delete the 6 files listed here:

  ~\Web Security\tomcat\bin\tcnative-1.dll

  ~\Web Security\tomcat\bin\tomcat-native.tar.gz

  ~\Web Security\tomcat\bin\x86-32\tcnative-1.dll

  ~\Websense\Web Security\rtm\tomcat\bin\tcnative-1.dll

  ~\Websense\Web Security\rtm\tomcat\bin\tomcat-native.tar.gz

  ~\Websense\Web Security\rtm\tomcat\bin\x86-32\tcnative-1.dll

  Restart ‘Websense TRITON - Web Security’ and ‘Websense RTM Server’.
- All Email Security and Email Security Gateway servers need to be patched, for the affected versions.
- All Data Security servers (except the Data protector and mobile agent) need to be patched, for all affected versions.

Please see the *Complete Product Tables*, page 2 for links to all instructions and fixes.

Please note the following urgent and critical information:

Complete Product Tables

Use the tables on the following pages to guide your steps as you repair the vulnerability on every affected server that runs Websense software.

Web security product impacts

Web Filter, Web Security, and Web Security Gateway products.

Web Products	Version	TRITON manager OpenSSL version	Content Gateway OpenSSL version	Affected? Recovery steps?
Web Filter Web Security	7.8.2	1.0.1e-fips	Not applicable	Yes, vulnerable. Hotfix for all Web Security modules except the TRITON infrastructure is here. TRITON management server infrastructure requires hotfix from this location. See these instructions for important missing step 3. *NOTE: After installing this Hotfix on the Windows Web Security management server, you MUST delete six tomcat files: Navigate to the Websense installation folder and Stop the Websense Triton – Web Security service and the Websense RTM Server. Then delete the 6 tomcat files listed here: ~\Web Security\tomcat\bin\ tcnative-1.dll ~\Web Security\tomcat\bin\ tomcat-native.tar.gz ~\Web Security\tomcat\bin\ x86-32\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tomcat-native.tar.gz ~\Websense\Web Security\rtm\ tomcat\bin\x86-32\tcnative-1.dll Start 'Websense TRITON - Web Security' and 'Websense RTM Server'.

Web Products	Version	TRITON manager OpenSSL version	Content Gateway OpenSSL version	Affected? Recovery steps?
Web Security Gateway Web Security Gateway Anywhere	7.8.2	1.0.1e-fips	1.0.1e (FIPS mode also uses the same version) No MDS, because Content Gateway handles SSL as well.	Yes, vulnerable. Hotfix for all Web Security modules except the TRITON infrastructure is here. Content Gateway hotfix is here. TRITON management server infra- structure requires hotfix from this location. See these instructions for important missing step 3. *NOTE: After you install this Hotfix on the Windows Web Security management server, you MUST delete six tomcat files: Navigate to the Websense installation folder and Stop the Websense Triton – Web Security service and the Websense RTM Server. Then delete the 6 tomcat files listed here: ~\Web Security\tomcat\bin\ tcnative-1.dll ~\Web Security\tomcat\bin\ tomcat-native.tar.gz ~\Web Security\tomcat\bin\ x86-32\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tomcat-native.tar.gz ~\Websense\Web Security\rtm\ tomcat\bin\x86-32\tcnative-1.dll Start ‘Websense TRITON - Web Security’ and ‘Websense RTM Server’.

Web Products	Version	TRITON manager OpenSSL version	Content Gateway OpenSSL version	Affected? Recovery steps?
Web Filter Web Security	7.8.1	1.0.1e-fips	Not applicable	Yes, vulnerable. Hotfix for all Web Security modules except the TRITON infrastructure is here. TRITON management server **infrastructure** requires hotfix from this location. See these instructions for important missing step 3. *NOTE: After you install this Hotfix on the Windows Web Security management server, you MUST delete six tomcat files: Navigate to the Websense installation folder and Stop the Websense Triton – Web Security service and the Websense RTM Server. Then delete the 6 tomcat files listed here: ~\Web Security\tomcat\bin\ tcnative-1.dll ~\Web Security\tomcat\bin\ tomcat-native.tar.gz ~\Web Security\tomcat\bin\ x86-32\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tomcat-native.tar.gz ~\Websense\Web Security\rtm\ tomcat\bin\x86-32\tcnative-1.dll Start 'Websense TRITON - Web Security' and 'Websense RTM Server'.

Web Products	Version	TRITON manager OpenSSL version	Content Gateway OpenSSL version	Affected? Recovery steps?
Web Security Gateway Web Security Gateway Anywhere	7.8.1	1.0.1e-fips	1.0.1e (FIPS mode also uses the same version) No MDS; Content Gateway handles SSL as well	Yes, vulnerable. Hotfix for all Web Security modules except the TRITON infrastructure is here. *NOTE: After you install this Hotfix on the Windows Web Security management server, you MUST delete six tomcat files: Navigate to the Websense installation folder and Stop the Websense Triton – Web Security service and the Websense RTM Server. Then delete the 6 tomcat files listed here: ~\Web Security\tomcat\bin\ tcnative-1.dll ~\Web Security\tomcat\bin\ tomcat-native.tar.gz ~\Web Security\tomcat\bin\ x86-32\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tcnative-1.dll ~\Websense\Web Security\rtm\ tomcat\bin\tomcat-native.tar.gz ~\Websense\Web Security\rtm\ tomcat\bin\x86-32\tcnative-1.dll Then, Start 'Websense TRITON - Web Security' and 'Websense RTM Server'. **Content Gateway** hotfix is here. TRITON management server **infrastructure** requires hotfix from this location. See these instructions for important missing step 3.
Web Filter Web Security	7.7.3	0.9.8	Not applicable	No impact.

Web Products	Version	TRITON manager OpenSSL version	Content Gateway OpenSSL version	Affected? Recovery steps?
Web Security Gateway Web Security Gateway Anywhere	7.7.3	0.9.8	0.9.8 MDS (embedded SSL engine) uses 1.0.1 FIPS-Mode-MDS uses 0.9.8	Yes, vulnerable if site is using non-FIPS* mode. Only Content Gateway in non-FIPS mode is vulnerable. Hotfix for Content Gateway is located here. No impact for TRITON manager or infrasturcture. No impact if your organization has previously enabled FIPS* mode. *FIPS = Federal Information Processing Standards for the U.S.Government, including cryptography standards. To be sure you understand the ramifications of using FIPS mode, please consult Websense Tech Support before enabling. This feature is enabled in the Content Gateway manager on the Configure > Security > FIPS Security page and is described in the embedded Help.
Web Filter Web Security	7.7.0	0.9.8	Not applicable	No impact.

Web Products	Version	TRITON manager OpenSSL version	Content Gateway OpenSSL version	Affected? Recovery steps?
Web Security Gateway Web Security Gateway Anywhere	7.7.0	0.9.8	0.9.8 MDS (embedded SSL engine) - 1.0.1 FIPS-Mode-MDS - 0.9.8	Yes, vulnerable if site is using non-FIPS* mode. **Content Gateway** hotfix is located here. No impact for TRITON manager or infrasturcture. No impact if your organization has previously enabled FIPS* mode. *FIPS = Federal Information Processing Standards for the U.S. Government, including cryptography standards. To be sure you understand the ramifications of using FIPS mode, please consult Websense Tech Support before enabling. This feature is enabled in the Content Gateway manager on the Configure > Security > FIPS Security page and is described in the embedded Help.
Web Fitler Web Security Web Security Gateway Web Security Gateway Anywhere	7.6.0 through 7.6.7 (any 7.6.x version)	0.9.8	Both Content Gateway and MDS use 0.9.8 No FIPS mode (Websense products introduced FIPS in 7.7.0)	No impact
Web Fitler Web Security Web Security Gateway Web Security Gateway Anywhere	7.5.x (Any 7.5.x version)	0.9.8	0.9.8	No impact
Web Fitler Web Security Web Security Gateway Web Security Gateway Anywhere	7.1.x (any 7.1.x version)	0.9.8	0.9.8	No impact

Data security product impacts

Websense Engineering has assigned IDs **DSS-4103** and **DSS-4104** to this vulnerability, as it pertains to Data Security Suite releases.

Data Product	Version	TRITON manager OpenSSL version	Infrastructure OpenSSL version	Affected?
Data Security Suite Note that DSS Protector continues to use OpenSSL 0.9.8.	7.8.2	1.0.1c	1.0.1c	Yes, vulnerable. Data Security server and Data Endpoint hotfix is here. An important Step 10 was added to the Data Security server Hotfix installation instructions after the release on April 18. See the full set of steps here. TRITON management server infrastructure requires hotfix from this location. See these instructions for important missing step 3. No DSS Protector versions are affected.
Data Endpoints (Windows and Mac OS X)	7.8.2	1.0.1c	1.0.1c	Yes, vulnerable. See line above.

Data Product	Version	TRITON manager OpenSSL version	Infrastructure OpenSSL version	Affected?
Data Security Suite Note that DSS Protector continues to use OpenSSL 0.9.8.	7.8.1	1.0.1c	1.0.1c	Yes, vulnerable. Data Security server and Data Endpoint hotfix is located here. TRITON management server infrastructure requires hotfix from this location. See these instructions for important missing step 3. No DSS Protector versions are affected.
Data Endpoints (Windows and Mac OS X)	7.8.1	1.0.1c	1.0.1c	Yes, vulnerable. See line above for the fix.
Data Security Suite Data Endpoint Protector Appliance	7.7.3 7.7.2 7.7.0 7.6.8 7.6.3 7.6.2 7.6.0. 7.5.x (all)	0.9.8	0.9.8	No impact

Email security product impacts

Websense Engineering has assigned ID **ESG-2962** to this vulnerability, as it pertains to Email Security Gateway products..

Email Product	Version	TRITON infrastructure OpenSSL version	Email OpenSSL version	Affected?
Email Security Gateway Email Security Gateway Anywhere Email Log Server	7.8.2 7.8	1.0.1c	1.0.1c	Yes, vulnerable. Appliance hotfix is available from the appliance console and on MyWebsense at this location. TRITON management server infrastructure requires hotfix from this location. See these instructions for important missing step 3. Please note that (on the TRITON management server, you need to stop the Email Security Gateway manager services, and then delete the following tomcat file from the folder shown here: \Websense\Email Security\ESG Manager\ tomcat\bin Delete: tcnative-1.dll
Email Security Gateway Email Security Gateway Anywhere Email Log Server	7.7.3	0.9.8	1.0.1c	Yes, vulnerable. Appliance hotfix is available from the appliance console and from this location on MyWebsense. Installation Instructions for the hotfix are here.

Email Product	Version	TRITON infrastructure OpenSSL version	Email OpenSSL version	Affected?
Email Security Gateway Email Security Gateway Anywhere	7.7.0 7.6.1 7.6.0	0.9.8	0.9.8	No impact.
Websense Email Security (WES)	7.3	Not applicable	1.0.1	Yes, vulnerable. Please see the hot-fix linked to this KBA.
Websense Email Security (WES)	7.2 and below	Not applicable	0.9.8	No impact.

V-Series and X-Series appliances

See the product matrices above for the impact on all software applications that are running on Websense appliances. Neither V-Series nor X-Series appliances make use of vulnerable OpenSSL libraries in any (underlying) appliance infrastructure modules.

Cloud security products not affected

Websense Cloud Security products in the Cloud services portal are not affected by this vulnerability.

i-Series and blueSKY

Note, however, that the on-premises i-Series appliance (i500) and blueSKY appliance (IQ-250) are affected at version 1.2.0.

Websense Engineering has assigned ID **TSAAS-1395** to this vulnerability, as it pertains to i-Series appliances images (version 1.2.0) for Cloud Web Security, and blueSKY appliances (version 1.2.0).

Note that i500 and IQ250 vulnerability is somewhat limited because the appliance terminates SSL only for serving block pages, quota pages, confirm pages, and auth pages (which do not require outbound SSL interaction with origin servers). SSL scanning is handled by Websense cloud services, which are not affected by the bug.

An updated version (1.2.1) for these appliances was posted on 21 April 2014 .

Overview of OpenSSL vulnerability

A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, due to incorrect memory handling in the TLS heartbeat extension.

For readers not familiar with OpenSSL, it is an Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength general purpose cryptography library. It is deployed in many scenarios, such as within email servers and VPN systems, and can be embedded within operating systems. Any system using a vulnerable version of OpenSSL is thus vulnerable to exploitation.

Several Websense products at version 7.7.3 or later use the vulnerable OpenSSL libraries. The tables below show specific impacts and workarounds.

Websense Cloud Security products in the Websense Cloud services portal are not affected.

What is the impact of this vulnerability?

OpenSSL versions 1.0.1 through 1.0.1f contain a flaw in the OpenSSL implementation of the TLS/DTLS heartbeat functionality. Version 1.0.1g corrects the flaw.

This flaw allows an attacker to retrieve the private memory of an application that uses the vulnerable OpenSSL library, in sections of 64K at a time.

Note that an attacker can repeatedly leverage the vulnerability to retrieve as many 64K sections of memory as are necessary to retrieve the intended secrets.

The sensitive information that may be retrieved using this vulnerability includes:

- Primary key material (secret keys)
- Secondary key material (user names and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- Collateral (memory addresses and content that can be leveraged to bypass exploit mitigations)

The first OpenSSL version affected by the Heartbleed bug is version 1.0.1, released in March 2012.

Websense Support has seen reports indicating that organizations not only need to get their infrastructure patched (so that potential future damage will not be incurred because of the vulnerability), but also that it is essential to replace or reissue certificates, to mitigate the risk from private keys stolen while the vulnerability existed in the wild. Changed certificates from all vendors need to be reviewed and replaced.

What will Websense Engineering provide for Websense products that use OpenSSL?

Corrections for affected products and affected versions were released to our customers on Friday, 18-April-2014.

Each correction has been posted to MyWebsense and to the Appliance download servers.

What should my team do now to protect our network?

Use recommended protections as quickly as possible. See Websense product tables below for additional details.

General protection steps

In general, sites are advised to update any software that uses the vulnerable OpenSSL libraries as quickly as possible. In addition:

- Upgrade OpenSSL to 1.0.1g or recompile your existing OpenSSL version with the option
  -DOPENSSL_NO_HEARTBEATS
- Revoke and reissue all Certificates from the past 2 years. (Note that any change to a Websense product should be done in consultation with your Websense Partner or Websense Technical Services.)
- Generate new private keys.
- Change passwords.
- Invalidate all session keys and cookies.

Possibly check anomalies between actual content length and what the header says.