Preliminary Evaluation of the OpenSSL Security Advisory (0.9.8 and 1.0.1)

Contents

Copyright

Preliminary Evaluation of the OpenSSL Security Advisory (0.9.8 and 1.0.1)

Pivotal Security Advisory	
Synopsis:	Pivotal Web Server, VMware vFabric Web Server, VMware vFabric Enterprise Ready Server updates of OpenSSL components
Issue date:	2014-06-13
Updated on:	2014-06-17
CVE	• *CVE-2014-0224* • *CVE-2014-3470* • *CVE-2014-0221* • *CVE-2014-0195* • *CVE-2014-0198* • *CVE-2010-5298* • *Other Issues*

Summary

This advisory describes Pivotal Web Server, VMware vFabric Web Server, and VMware vFabric Enterprise Ready Server (ERS) updates of OpenSSL components

SSL/TLS MITM vulnerability (CVE-2014-0224)

Description

An attacker using a carefully-crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.

The attack can only be performed between a vulnerable client *and* server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1. Users of OpenSSL servers earlier than 1.0.1 are advised to upgrade as a precaution.

- OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za.
- OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m.
- OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Thanks to KIKUCHI Masashi (Lepidum Co. Ltd.) for discovering and researching this issue. This issue was reported to OpenSSL on 1st May 2014 via JPCERT/CC.

The fix was developed by Stephen Henson of the OpenSSL core team partly based on an original patch from KIKUCHI Masashi.

The scope of this vulnerability is described in *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224*.

Pivotal Evaluation

Product	Affected Versions	Severity
VMware vFabric Web Server	5.0.0-5.0.2	Moderate
VMware vFabric Web Server	5.1.0-5.3.4	Important
Pivotal Web Server	5.4.0	Important
VMware vFabric ERS	4.0.3 (including SP2)	Moderate

Risk by Product Version

Pivotal Web Server, vFabric Web Server, and vFabric ERS offer mod_ssl using the bundled OpenSSL library for HTTPS TLS server termination. OpenSSL is also used in these products as an HTTPS client for proxied content, for LDAPS authentication through OpenLDAP, and in vFabric Web Server versions 5.0-5.3 for the native license client connection to the vFabric License Server. These client back-end connections are typically routed through intranet topography under the control of the enterprise, limiting the potential risks of MITM attacks against the products operating as a TLS client.

vFabric ERS packages shipped OpenSSL 0.9.8 and as an HTTPS server appears not to be vulnerable. ERS configured to use HTTPS proxy connections to vulnerable back-end servers presents a Moderate Severity risk. If ERS is used as a proxy server with HTTPS connections to vulnerable back-end servers and that back-end traffic is routed outside of the control of the enterprise organization, that combination should be considered a more significant risk. As the EOL period for this product occurs July 1st, security patches are now issued for Critical defects only. End of General Support for ERS is July 1 2014, after which no further patches will be issued.

vFabric Web Server releases from 5.0.0 through 5.0.2 shipped OpenSSL version 0.9.8, and as an HTTPS server appears not to be vulnerable. Where configured to use HTTPS proxy connections to vulnerable back-end servers, there appears to be a Moderate Severity risk. When used as a proxy server with HTTPS connections to vulnerable back-end servers, where that back-end traffic is routed outside of the control of the enterprise organization, that combination should be considered a more significant risk. Vulnerabilities previously corrected after release 5.0.2 require all users to update to the most recent release. These specific versions cannot be patched.

vFabric Web Server releases from 5.1.0 through 5.3.4 and Pivotal Web Server release 5.4.0 shipped OpenSSL 1.0.1, and appear to present an Important Severity risk, both as HTTPS servers and as HTTPS clients in the situation that HTTPS reverse proxy to originate server traffic passes over an untrusted network.

Recommendations

Pivotal recommends that all vFabric ERS, vFabric Web Server and Pivotal Web Server instances be updated to Pivotal Web Server 5.4.1 to avoid weakened public internet routed traffic from similarly affected user agents. Pivotal Web Server 5.4.1 builds are progressing now and a release is expected imminently. This update will be followed by an alternative patch to only the OpenSSL library files shipped with vFabric Web Server releases 5.1.0 through 5.3.4 once regression testing can be completed. See *Applying the vFabric Web Server OpenSSL 1.0.1h Patch* on page 5 for instructions. This notification will be updated upon release. Upgrading to Pivotal Web Server 5.4.1 is strongly recommended over applying this OpenSSL patch. In the meantime, customers are advised to prioritize the updates of any outward-facing, publicly-routed server traffic over internally-routed servers using trusted networks.

Applying the vFabric Web Server OpenSSL 1.0.1h Patch

The provided patch should be applied immediately to fix the critical security vulnerability reported in CVE-2014-0224.

This patch updates the OpenSSL library to the following version:

- OpenSSL 1.0.1h

  Important: The OpenSSL 1.0.1h patch does *not* require the previously-released OpenSSL 1.0.1g patch as a prerequisite.

The Common Vulnerabilities and Exposures project (*http://cve.mitre.org/*) has assigned the name CVE-2014-0224 to this issue.

The **Replace with / Apply Patch** column in the following table lists the action required to remediate the vulnerabilities in each release.

Pivotal Product	Product Version	Running On	Replace with / Apply Patch
vFabric Web Server	5.1.0 to 5.3.x	Windows (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-x86-windows.zip.exe
vFabric Web Server	5.1.0 to 5.3.x	Windows (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1h-x64-windows.zip.exe
vFabric Web Server	5.1.0 to 5.3.x	Linux (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-x86-linux-glibc2.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Linux (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1h-x86_64-linux-glibc2.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Solaris 10 (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-x86-solaris-10.x.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Solaris 10 (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1h-x86_64-solaris-10.x.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Linux (PPC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-ppc-linux-glibc2.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Linux (PPC, 64-bit)	vfabric-web-server-patch-openssl-1.0.1h-ppc64-linux-glibc2.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	HP UX (ia64, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-ia64-hp-hpux-11.23.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	HP UX (ia64, 64-bit	vfabric-web-server-patch-openssl-1.0.1h-ia64-hp-hpux64-11.23.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	IBM AIX (PPC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-

Pivotal Product	Product Version	Running On	Replace with / Apply Patch
			powerpc-ibm-aix-6.1.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	IBM AIX (PPC, 64-bit)	vfabric-web-server-patch-openssl-1.0.1h-powerpc64-ibm-aix-6.1.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Linux (S390, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-s390-linux-glibc2.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Linux (S390x, 64-bit)	vfabric-web-server-patch-openssl-1.0.1h-s390x-linux-glibc2.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Solaris (SPARC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1h-sparc-sun-solaris-10.x.zip.sfx
vFabric Web Server	5.1.0 to 5.3.x	Solaris (SPARCv9, 64-bit)	vfabric-web-server-patch-openssl-1.0.1h-sparcv9-sun-solaris-10.x.zip.sfx

Solution

1. Download the appropriate patch file for your operating system and architecture. To download the patch file appropriate for your operating system and architecture, please visit *http://download.gopivotal.com/webserver/5.x_patch/index.html*.
2. Review the contents of the /opt/vmware/vfabric-web-server directory on all your systems for one or more **httpd-2.2.x.y-{32/64}** binary packages. (Note that **httpd-2.2** is simply a symlink to a specific binary version.)
3. For each directory that contains a **httpd-2.2.x.y** binary package, unpack (or on Windows, execute) the patch file into that directory. For example, on Linux or Unix based-systems:
   a. Change directories to the affected directory:

      cd /opt/vmware/vfabric-web-server/*instance-dir/* httpd-2.2/
   b. Copy the downloaded patch file into the current directory.
   c. Change the permissions of the downloaded ZIP file to make it executable.

      chmod +x vfabric-web-server-patch-openssl-1.0.1h-*version* .zip.sfx
   d. Self-extract the files from the downloaded patch file.

      ./vfabric-web-server-patch-openssl-1.0.1h-*version* .zip.sfx -o

      Note: If necessary, use the ‘ -o ’ switch to overwrite existing files without prompting.
   e. Verify that the package has replaced the OpenSSL command line tool and all OpenSSL components consumed by the httpd runtime. The new OpenSSL components should update to revision 1.0.1.g.

      On Linux or Unix-based systems, the following files are replaced:

      - bin/openssl
      - lib/libssl.so.1.0.0
      - lib/libcrypto.so.1.0.0

- lib/engines/lib{engine*}.so
- ssl/openssl.cnf

On Windows systems, the following files are replaced:

- bin/openssl.exe
- bin/ssleay32.dll
- bin/libeay32.dll
- bin/engines/{engine*}.dll
- ssl/openssl.cnf

4. After you have patched your system, restart the server.
5. Restart your vFabric Web Server instances and verify that each instance is using the upgraded version of OpenSSL. For each instance, check `error.log` under *vfabric-web-server-install-dir/instance-dir/* logs/ for a message similar to the following:

```
[Tue Apr 08 14:37:06 2014] [info] mod_ssl/2.2.26 compiled against
Server: Apache/2.2.26, Library: OpenSSL/1.0.1e-fips [Tue Apr 08 14:37:06
2014] [notice] Apache/2.2.26 (Unix) vFabric/5.3.3 vFabricLicense/5.3.3
mod_ssl/2.2.26 OpenSSL/1.0.1g -fips DAV/2 mod_bmx/0.9.4 configured --
resuming normal operations
```

Alternately, you can check the HTTP headers returned by the Web Server instance by using curl. For example:

```
% curl -I http://hostname
HTTP/1.1 200 OK
Date: Tue, 08 Apr 2014 21:36:58 GMT
Server: Apache/2.2.26 (Unix) vFabric/5.3.3 vFabricLicense/5.3.3
 mod_ssl/2.2.26 OpenSSL/1.0.1g-fips DAV/2 mod_bmx/0.9.4
Last-Modified: Tue, 08 Apr 2014 21:11:52 GMT
ETag: "294db9-b57-4f68e6ed3b600"
Accept-Ranges: bytes
Content-Length: 2903
Content-Type: text/html
```

6. Finally, after you have patched and restarted all your servers, you should review your systems for what may have been compromised and take the appropriate steps. For example, you may need to provision new keys and certificates, revoke old server certificates, change any passwords or close any long running sessions. Work with your security team to analyze all security changes required by your systems.

   You may also want to periodically check *http://www.kb.cert.org/vuls/id/720951* for up-to-date information on known impact.

References

- *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224*
- *http://www.openssl.org/news/vulnerabilities.html*
- *http://www.kb.cert.org/vuls/id/978508*

Anonymous ECDH denial of service (CVE-2014-3470)

Description

OpenSSL TLS clients enabling anonymous ECDH ciphersuites are subject to a denial of service attack.

- OpenSSL 0.9.8 users should upgrade to 0.9.8za.

- OpenSSL 1.0.0 users should upgrade to 1.0.0m.
- OpenSSL 1.0.1 users should upgrade to 1.0.1h.

Thanks to Felix Gröbert and Ivan Fratri# at Google for discovering this issue. This issue was reported to OpenSSL on 28th May 2014.The fix was developed by Stephen Henson of the OpenSSL core team.

The scope of this vulnerability is described in *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3470*.

Pivotal Evaluation

Product	Affected Versions	Severity
VMware vFabric Web Server	5.3.3, 5.3.4	Low
Pivotal Web Server	5.4.0	Low

ERS httpd never shipped an ECC-enabled OpenSSL.

vFabric Web Server did not utilize this feature until release 5.3.3. Release 5.3.3 and 5.3.4 and Pivotal Web Server 5.4.0 do permit the user to enable ECDH ciphers. ECDH key exchange is not enabled out of the box.

DTLS recursion flaw (CVE-2014-0221)

Description

By sending an invalid DTLS handshake to an OpenSSL DTLS client the code can be made to recurse eventually crashing in a DoS attack. Only applications using OpenSSL as a DTLS client are affected.

- OpenSSL 0.9.8 users should upgrade to 0.9.8za.
- OpenSSL 1.0.0 users should upgrade to 1.0.0m.
- OpenSSL 1.0.1 users should upgrade to 1.0.1h.

Thanks to Imre Rad (Search-Lab Ltd.) for discovering this issue. This issue was reported to OpenSSL on 9th May 2014.

The fix was developed by Stephen Henson of the OpenSSL core team.

The scope of this vulnerability is described in *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0221*.

Pivotal Evaluation

Product	Affected Versions	Severity
VMware vFabric Web Server	None	N/A
Pivotal Web Server	None	N/A
vFabric ERS httpd	None	N/A

Pivotal (or vFabric or ERS httpd) Web Server products do not employthe DTLS protocol.

DTLS invalid fragment vulnerability (CVE-2014-0195)

Description

A buffer overrun attack can be triggered by sending invalid DTLS fragments to an OpenSSL DTLS client or server. This is potentially exploitable to run arbitrary code on a vulnerable client or server.

Only applications using OpenSSL as a DTLS client or server affected.

- OpenSSL 0.9.8 users should upgrade to 0.9.8za.
- OpenSSL 1.0.0 users should upgrade to 1.0.0m.
- OpenSSL 1.0.1 users should upgrade to 1.0.1h.

Thanks to Jüri Aedla for reporting this issue. This issue was reported to OpenSSL on 23rd April 2014 via HP ZDI.

The fix was developed by Stephen Henson of the OpenSSL core team.

The scope of this vulnerability is described in *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0195*.

Pivotal Evaluation

Product	Affected Versions	Severity
VMware vFabric Web Server	None	N/A
Pivotal Web Server	None	N/A
vFabric ERS httpd	None	N/A

Pivotal (or vFabric or ERS httpd) Web Server products do not employ the DTLS protocol.

SSL_MODE_RELEASE_BUFFERS NULL pointer dereference (CVE-2014-0198)

Description

A flaw in the do_ssl3_write function can allow remote attackers to cause a denial of service via a NULL pointer dereference. This flaw only affects OpenSSL 1.0.0 and 1.0.1 where SSL_MODE_RELEASE_BUFFERS is enabled, which is not the default and not common.

- OpenSSL 1.0.0 users should upgrade to 1.0.0m.
- OpenSSL 1.0.1 users should upgrade to 1.0.1h.

This issue was reported in public. The fix was developed by Matt Caswell of the OpenSSL development team.

The scope of this vulnerability is described in *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0198*.

Pivotal Evaluation

Product	Affected Versions	Severity
VMware vFabric Web Server	None	N/A
Pivotal Web Server	None	N/A
vFabric ERS httpd	None	N/A

Pivotal (and vFabric and ERS httpd) Web Server products do not enable the SSL_MODE_RELEASE_BUFFERS facility.

SSL_MODE_RELEASE_BUFFERS session injection or denial of service (CVE-2010-5298)

Description

A race condition in the ssl3_read_bytes function can allow remote attackers to inject data across sessions or cause a denial of service.

This flaw only affects multithreaded applications using OpenSSL 1.0.0 and 1.0.1, where SSL_MODE_RELEASE_BUFFERS is enabled, which is not the default and not common.

- OpenSSL 1.0.0 users should upgrade to 1.0.0m.
- OpenSSL 1.0.1 users should upgrade to 1.0.1h.

This issue was reported in public.

The scope of this vulnerability is described in *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5298*.

Pivotal Evaluation

Product	Affected Versions	Severity
VMware vFabric Web Server	None	N/A
Pivotal Web Server	None	N/A
vFabric ERS httpd	None	N/A

Pivotal (and vFabric and ERS httpd) Web Server products do not enable the SSL_MODE_RELEASE_BUFFERS facility.

Other Issues

Description

OpenSSL 1.0.0m and OpenSSL 0.9.8za also contain a fix for CVE-2014-0076: Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack" reported by Yuval Yarom and Naomi Benger. This issue was previously fixed in OpenSSL 1.0.1g.

The scope of this vulnerability is described in *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0076*.

Pivotal Evaluation

Product	Affected Versions	Severity
VMware vFabric Web Server	5.3.3	Low

ERS httpd never shipped an ECC-enabled OpenSSL. vFabric Web Server did not utilize this feature until release 5.3.3. Release 5.3.3 based on httpd 2.2.26 did enable ECC cryptography and included the vulnerable OpenSSL 1.0.1e. VMware vFabric Web Server 5.3.4 and Pivotal Web Server 5.4.0 shipped with the corrected OpenSSL 1.0.1g. ECDSA keys are not deployed out of the box.

Contacts

For more information, visit *http://www.gopivotal.com/security* or contact security@gopivotal.com.