Security Advisory on Updates to Pivotal / VMware vFabric Web Server

Pivotal Security Advisory	
Synopsis:	Pivotal / VMware vFabric Web Server updates of OpenSSL components
Issue date:	2014-10-27
Updated on:	2014-10-27
CVE	CVE-2014-3513

Summary

This advisory describes Pivotal / VMware vFabric Web Server security updates of OpenSSL components. The Web Server patch (provided by Pivotal) should be applied immediately to fix the security vulnerability reported in CVE-2014-3513. The scope of this important vulnerability is described in *https://www.openssl.org/news/secadv_20141015.txt*.

Relevant Releases

This advisory applies to the following releases:

- Pivotal Web Server 6.0.0 to 6.0.1
- Pivotal Web Server 5.4.0 to 5.4.2
- VMware vFabric Web Server 5.3.x
- VMware vFabric Web Server 5.2.x
- VMware vFabric Web Server 5.1.x

Note: The VMware vFabric releases were previously released on the VMware downloads site.

Problem Description

Pivotal / VMware vFabric Web Server requires an update to resolve security issues found in the OpenSSL library that it uses.

Mitigation

Pivotal recommends upgrading to one of the following Pivotal Web Server releases:

- Pivotal Web Server 5.4.3 or later
- Pivotal Web Server 6.0.2 or later

These releases include OpenSSL 1.0.1j or later.

Alternatively, apply the provided Web Server patch immediately to fix the security vulnerability reported in CVE-2014-3513.

This patch updates the OpenSSL library to the following version:

- OpenSSL 1.0.1j

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2014-3513 to this issue.

The **Replace with / Apply Patch** column in the following table lists the action required to remediate the vulnerabilities in each release, if a solution is available.

Pivotal Product	Product Version	Running On	Replace with / Apply Patch
vFabric Web Server	5.1.x to 5.3.x	Windows (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-x86-windows.zip.exe
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Windows (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1j-x64-windows.zip.exe
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Linux (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-x86-linux-glibc2.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Linux (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1j-x86_64-linux-glibc2.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Solaris 10 (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-x86-solaris-10.x.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		

Pivotal Product	Product Version	Running On	Replace with / Apply Patch
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Solaris 10 (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1j-x86_64-solaris-10.x.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Linux (PPC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-ppc-linux-glibc2.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Linux (PPC, 64-bit)	vfabric-web-server-patch-openssl-1.0.1j-ppc64-linux-glibc2.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	HP UX (ia64, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-ia64-hp-hpux-11.23.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	HP UX (ia64, 64-bit	vfabric-web-server-patch-openssl-1.0.1j-ia64-hp-hpux64-11.23.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	IBM AIX (PPC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-powerpc-ibm-aix-6.1.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	IBM AIX (PPC, 64-bit)	vfabric-web-server-patch-openssl-1.0.1j-powerpc64-ibm-aix-6.1.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		

Pivotal Product	Product Version	Running On	Replace with / Apply Patch
vFabric Web Server	5.1.x to 5.3.x	Linux (S390, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-s390-linux-glibc2.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Linux (S390x, 64-bit)	vfabric-web-server-patch-openssl-1.0.1j-s390x-linux-glibc2.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Solaris (SPARC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1j-sparc-sun-solaris-10.x.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		
vFabric Web Server	5.1.x to 5.3.x	Solaris (SPARCv9, 64-bit)	vfabric-web-server-patch-openssl-1.0.1j-sparcv9-sun-solaris-10.x.zip.sfx
Pivotal Web Server	5.4.0 to 5.4.2		
	6.0.0 to 6.0.1		

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.pivotal.io/webserver/5.x_patch/index.html*.

   Note: These instructions refer to the OpenSSL 1.0.1j patch. When this alert was written, that was the latest patch version. A later patch may supercede this version. Download the current patch to take advantage of the latest updates.

2. Review the contents of the `/opt/pivotal/webserver` (Pivotal) or `/opt/vmware/vfabric-web-server` (VMware) directory on all your systems for one or more **httpd-2.2.x.y-{32/64}** binary packages.

   Note: **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/ (VMware)
   - cd /opt/pivotal/webserver/ httpd-2.2/ (Pivotal 5.4.x)
   - cd /opt/pivotal/webserver/httpd-2.4/ (Pivotal 6.0.x)

   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-1.0.1j-*version* .zip.sfx

d. Self-extract the files from the downloaded patch file.

./vfabric-web-server-patch-openssl-1.0.1j-*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 1.0.1j.

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 Web Server instances and verify that each instance is using the upgraded version of OpenSSL. For each instance, check error.log under *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/1.0.1j** -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/1.0.1j-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.

Additional Recommendations

In additional to applying the patch, Pivotal recommends that you remove explicit support for SSLv3 in the SSLProtocol directive, as well as insecure block ciphers that are also subject to padding attacks.

Disabling this support will make your site inaccessible to some end users with older browsers that require this support.

References

- *https://www.openssl.org/news/secadv_20141015.txt*
- *http://www.openssl.org/news/vulnerabilities.html*

Contacts

For more information, visit *http://www.pivotal.io/security* or contact security@pivotal.io.