Security Advisory on Critical Updates for vFabric Web Server

Contents

Copyright

Security Advisory on Critical Updates to vFabric Web Server

Pivotal Security Advisory	
Synopsis:	vFabric Web Server updates of OpenSSL components
Issue date:	2014-04-09
Updated on:	2014-06-17
CVE	CVE-2014-0160

Summary

This advisory describes vFabric Web Server security updates of OpenSSL components. The vFabric Web Server patch (provided by Pivotal) should be applied immediately to fix the critical security vulnerability reported in CVE-2014-0160. The scope of this important vulnerability is described in *http://www.kb.cert.org/vuls/id/720951*.

Relevant Releases

This advisory applies to the following releases:

- VMware vFabric Web Server 5.3.x
- VMware vFabric Web Server 5.2.x
- VMware vFabric Web Server 5.1.x

Note:

- The advisory does not apply to VMware vFabric Web Server 5.0.x. These versions are not affected by the vulnerability described in CVE-2014-0160.
- The VMware vFabric releases were previously released on the VMware downloads site.

Problem Description

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

Mitigation

The provided vFabric Web Server patch should be applied immediately to fix the critical security vulnerability reported in CVE-2014-0160.

This patch updates the OpenSSL library to the following version:

- OpenSSL 1.0.1g

Important: The OpenSSL 1.0.1g patch is superceded by the OpenSSL 1.0.1h patch. Download and install that patch instead. See *http://webserver.docs.gopivotal.com/security/CVE-2014-0224-Advisory.pdf* for the patch installation instructions.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2014-0160 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-1.0.1g-x86-windows.zip.exe
vFabric Web Server	5.1.x to 5.3.x	Windows (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1g-x64-windows.zip.exe
vFabric Web Server	5.1.x to 5.3.x	Linux (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1g-x86-linux-glibc2.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Linux (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1g-x86_64-linux-glibc2.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Solaris 10 (x86, 32-bit)	vfabric-web-server-patch-openssl-1.0.1g-x86-solaris-10.x.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Solaris 10 (x86, 64-bit)	vfabric-web-server-patch-openssl-1.0.1g-x86_64-solaris-10.x.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Linux (PPC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1g-ppc-linux-glibc2.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Linux (PPC, 64-bit)	vfabric-web-server-patch-openssl-1.0.1g-ppc64-linux-glibc2.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	HP UX (ia64, 32-bit)	vfabric-web-server-patch-openssl-1.0.1g-ia64-hp-hpux-11.23.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	HP UX (ia64, 64-bit	vfabric-web-server-patch-openssl-1.0.1g-ia64-hp-hpux64-11.23.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	IBM AIX (PPC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1g-powerpc-ibm-aix-6.1.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	IBM AIX (PPC, 64-bit)	vfabric-web-server-patch-openssl-1.0.1g-

Pivotal Product	Product Version	Running On	Replace with / Apply Patch
			powerpc64-ibm-aix-6.1.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Linux (S390, 32-bit)	vfabric-web-server-patch-openssl-1.0.1g-s390-linux-glibc2.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Linux (S390x, 64-bit)	vfabric-web-server-patch-openssl-1.0.1g-s390x-linux-glibc2.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Solaris (SPARC, 32-bit)	vfabric-web-server-patch-openssl-1.0.1g-sparc-sun-solaris-10.x.zip.sfx
vFabric Web Server	5.1.x to 5.3.x	Solaris (SPARCv9, 64-bit)	vfabric-web-server-patch-openssl-1.0.1g-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*.

   Important: The OpenSSL 1.0.1g patch is superceded by the OpenSSL 1.0.1h patch. Download and install that patch instead. See *http://webserver.docs.gopivotal.com/security/CVE-2014-0224-Advisory.pdf* for the patch installation instructions.
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-1.0.1g-*version* .zip.sfx
   d. Self-extract the files from the downloaded patch file.

      ./vfabric-web-server-patch-openssl-1.0.1g-*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-2014-0160*
- *http://www.openssl.org/news/vulnerabilities.html*
- *http://www.kb.cert.org/vuls/id/720951*
- *http://heartbleed.com/*

Contacts

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