OpenBSD DoS vulnerability

Security Advisory **Criticality** High

Advisory Released On 08-Feb-2017

Impact

It's possible to DoS the remote server by requesting a file over and over by specifying a custom file range.

Solution

Refer to the "Solution" section below

Summary

aeCERT has researched and found about a new bug in OpenBSD web servers. OpenBSD and two of its SSL libraries need patches against a pair of denial-of-service bugs that can crash Web-facing servers.

Threat Details

A single renegotiation thread can soak up 70 per cent of CPU cycles, meaning if the attacker fires multiple renegotiation threads at the target, the daemon will crash, and “there is no trace of such attacks in the httpd logs.
The second, which has been given the common vulnerabilities and exposures number CVE-2017-5850, is a memory exhaustion bug, again in the HTTP daemon. “Requesting file using a file-range will result in having a httpd process doing a full malloc() of the requested file, It appears the entry is not correctly free(). ("Malloc()" and "free()" are memory management calls in the standard C library).
Hence why it's possible to DoS the remote server by requesting a file over and over by specifying a custom range. The other requirement for this to work is that the attacker has to find a file that is greater than 10MB in size for it to be served by the victim's machine.

Solution

OpenBSD has responded to the two issues. The memory exhaustion bug is dealt with in bug fixes for version 6.0, or for version 5.9. Refer to the below URLs for more information:

• Version 6.0: https://ftp.openbsd.org/pub/OpenBSD/patches/6.0/common/017_httpd.patch.sig
• Version 5.9: https://ftp.openbsd.org/pub/OpenBSD/patches/5.9/common/034_httpd.patch.sig
The fix is in patches in the SSL and TLS libraries so sysadmins can block client-initiated renegotiation.

Contact Us

aeCERT

P.O. Box 116688 Dubai, United Arab Emirates

Tel	(+971) 4 230 0003
Fax	(+971) 4 230 0100
Email	info@aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT@aeCERT.ae