Inspector ScanDAll Reports

Here is the list of open ports on scanned system. (Scanned Host is:485646)

For port: 80/tcp CVE-id is: CVE-2009-4355

CVSS Score: 5.0

Description and Details:

Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.

For port: 443/tcp CVE-id is: CVE-2009-4355

CVSS Score: 5.0

Description and Details:

Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.

For port: 8080/tcp CVE-id is: CVE-2018-1312

CVSS Score: 6.8

Description and Details:

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

==

Solution

Firstly, most of attacks occur because of using the old versions of the services. You must try to update your applications as frequently as possible. Also, you can and should disable unneeded services on your systems. Like reducing the number of entry points in your house, the more enrty points you eliminate the fewer places an intruder can break in.

[This work is made by A. Murzaeva, C. Yilmaz and Z. Mutlu]