Report

Found 3 critical vulnerability in website

URL :https:// zero.webappsecurity.com/

Version :0.9.8e and 3.0.1(in this branch)

OWASP 2013&2017 : A9 Certification

# Vulnerabilities : Out-of-date Version (Tomcat)

# Out-of-date Version(Apache)

# Out-of-date Version(OpenSSL)

Report on Out-of-date Version(OpenSSL) vuln:

Details

* .Level: Critical
* Netsparker identified that the above website is using an out-date-version of OpenSSL
* Since this is an old version of the software, it may be vulnerable to attacks.
* Remedy : upgrade your openSSL to latest version.

Some Vulnerabilities Netsparker has found :

OpenSSL Resource Management Errors Vulnerability

* d1\_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.
* Double free vulnerability in d1\_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

OpenSSL Cryptographic Issues Vulnerability

* The ssl3\_send\_client\_key\_exchange function in s3\_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.
* The ssl3\_send\_client\_key\_exchange function in s3\_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

* While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

Netspaker has found 10s and 20s of vulnerabilities in this website.

These are the some vulnerabilities of those.

From these vulnerabilities a hacker can easily hack the website and steal the information that is sensitive to you .

Reason &Suggestions

All the softwares are old version and are very vulnerable to so many attacks.

I suggest that you upgrade your softwares to higher version and secured version.

Screenshots:











