Vulnerability report

Domain: https://zero.webappsecurity.com/

Vulnerability name: Out-of-date Version (OpenSSL**)**

Level of severity: Critical

Vulnerability Details

With help of net sparker automatic scanner we have come to know that this domain is using an old version of the OpenSSL which is “0.9.8e” and the latest version is “1.1.1k”

Impact of this vulnerability:

This particular version has exposed too much vulnerability such as CVE-2016-0703, CVE-2015-3195, CVE-2015-1792, etc. This version had contains 5 critical and 107 other vulnerabilities

Proof of this vulnerability:

This was http request was made by net sparker:

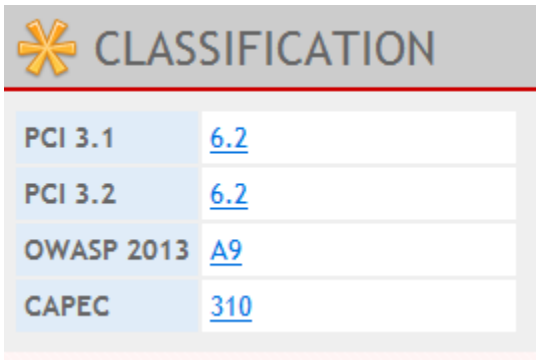
```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Cache-Control: no-cache
Referer: https://zero.webappsecurity.com/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

This was the response we got:

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Fri, 13 Aug 2021 17:25:00 GMT
ETag: "24c22-2c-44adde00"
```

As highlighted it shows the version of openSSL which is not secure at all.

Classification: According to Net sparker



Known Vulnerability in this version:

[1] OpenSSL Resource Management Errors Vulnerability (CVE-2012-1165)

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP

address blocks or (2) Autonomous System (AS) identifiers.

- CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	399

[2] OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (CVE-2012-2110)

The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

- CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Overflow Memory corruption
CWE ID	119

Mitigation for this vulnerability:

We need to keep our openSSL updated to avoid such vulnerability. It is a good practice to keep all the service’s and tools updated.