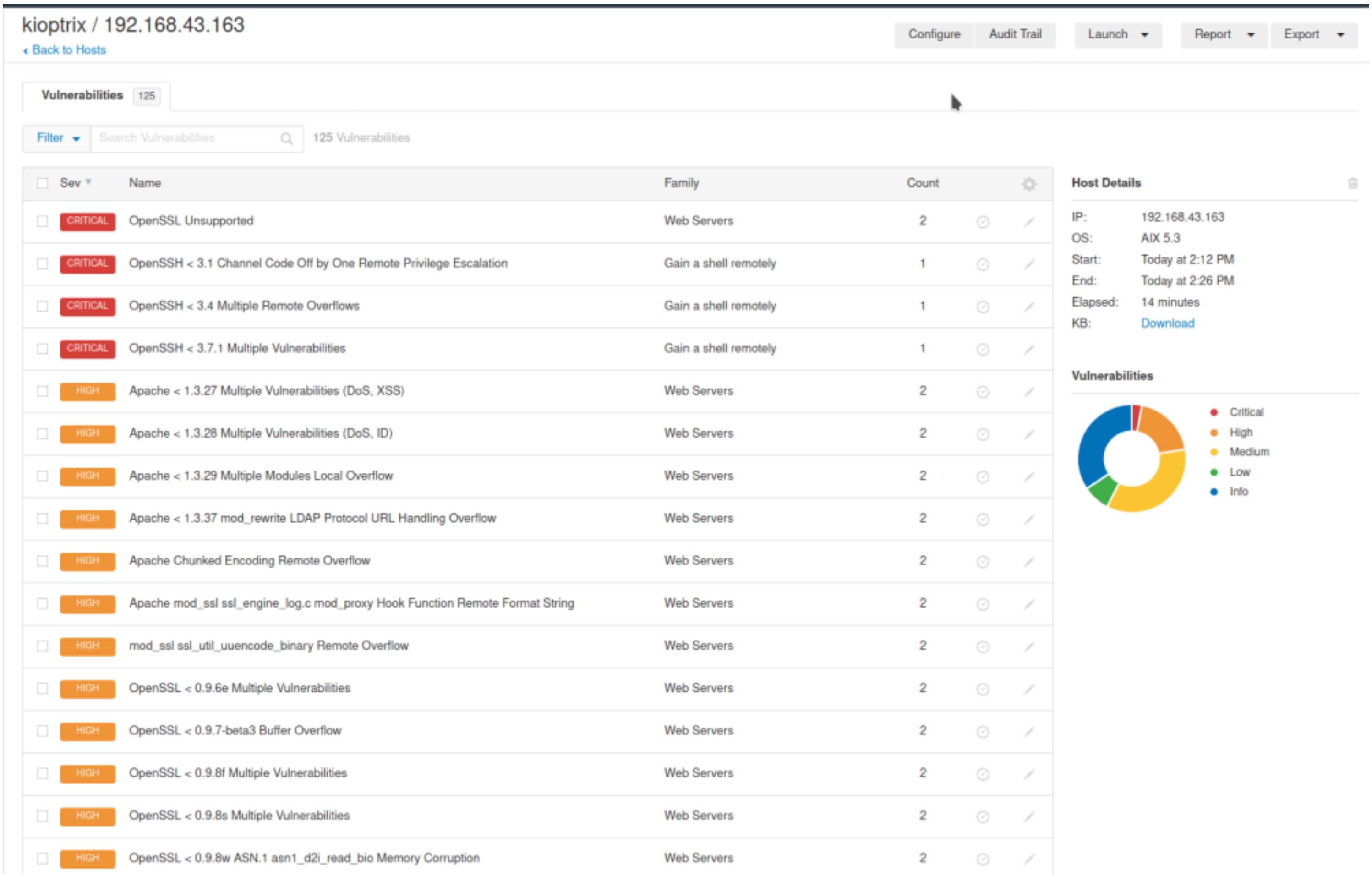
## *advanced_scanners*



kioptrix / 192.168.43.163

‹ Back to Hosts

Vulnerabilities 125

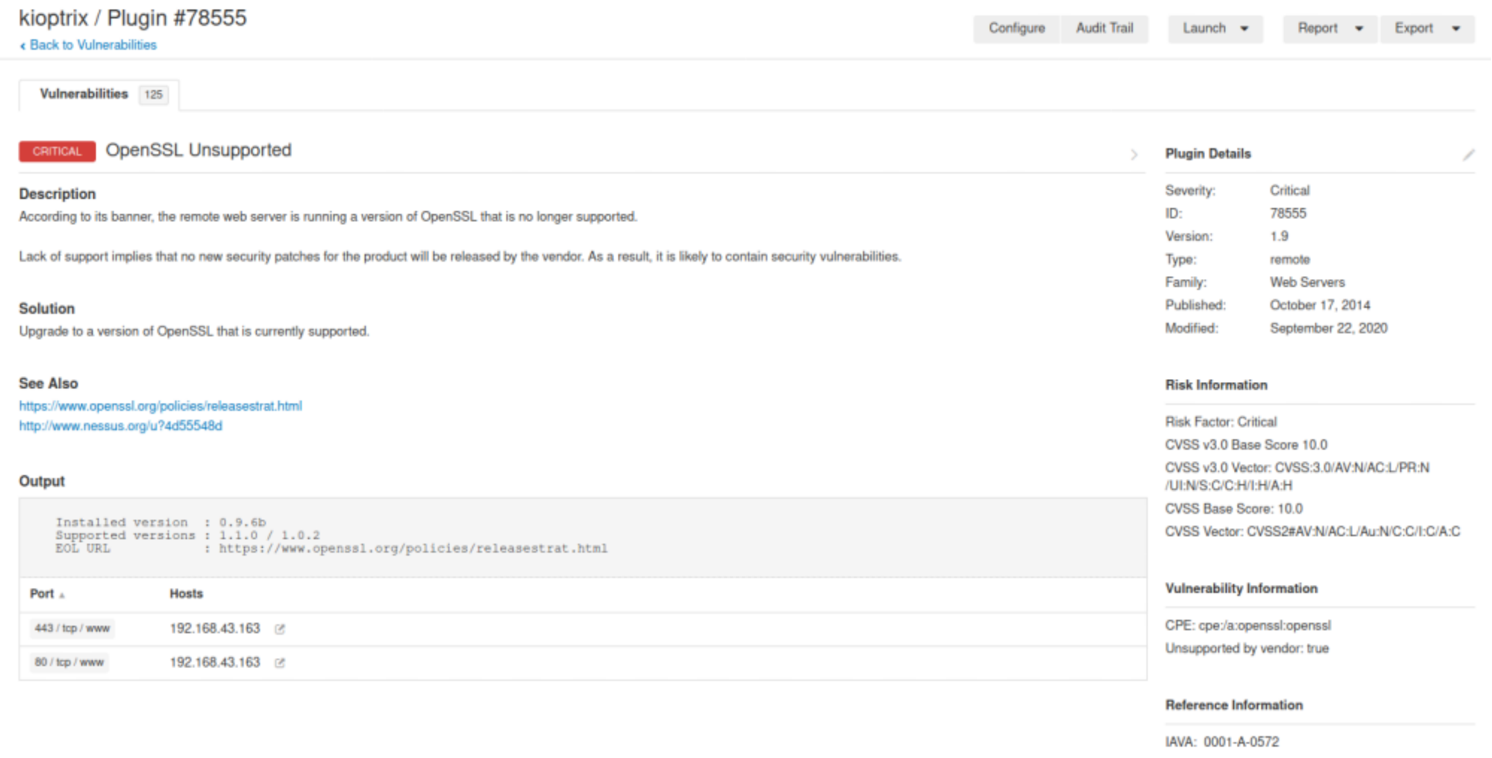
125 Vulnerabilities

| ☐ | Sev | Name | Family | Count |
|---|---|---|---|---|
| ☐ | CRITICAL | OpenSSL Unsupported | Web Servers | 2 |
| ☐ | CRITICAL | OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation | Gain a shell remotely | 1 |
| ☐ | CRITICAL | OpenSSH < 3.4 Multiple Remote Overflows | Gain a shell remotely | 1 |
| ☐ | CRITICAL | OpenSSH < 3.7.1 Multiple Vulnerabilities | Gain a shell remotely | 1 |
| ☐ | HIGH | Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS) | Web Servers | 2 |
| ☐ | HIGH | Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID) | Web Servers | 2 |
| ☐ | HIGH | Apache < 1.3.29 Multiple Modules Local Overflow | Web Servers | 2 |
| ☐ | HIGH | Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow | Web Servers | 2 |
| ☐ | HIGH | Apache Chunked Encoding Remote Overflow | Web Servers | 2 |
| ☐ | HIGH | Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String | Web Servers | 2 |
| ☐ | HIGH | mod_ssl ssl_util_uuencode_binary Remote Overflow | Web Servers | 2 |
| ☐ | HIGH | OpenSSL < 0.9.6e Multiple Vulnerabilities | Web Servers | 2 |
| ☐ | HIGH | OpenSSL < 0.9.7-beta3 Buffer Overflow | Web Servers | 2 |
| ☐ | HIGH | OpenSSL < 0.9.8f Multiple Vulnerabilities | Web Servers | 2 |
| ☐ | HIGH | OpenSSL < 0.9.8s Multiple Vulnerabilities | Web Servers | 2 |
| ☐ | HIGH | OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption | Web Servers | 2 |

**Host Details**

| | |
|---|---|
| IP: | 192.168.43.163 |
| OS: | AIX 5.3 |
| Start: | Today at 2:12 PM |
| End: | Today at 2:26 PM |
| Elapsed: | 14 minutes |
| KB: | Download |

**Vulnerabilities**



kioptrix / Plugin #78555

‹ Back to Vulnerabilities

Vulnerabilities 125

CRITICAL OpenSSL Unsupported

**Description**

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**Solution**

Upgrade to a version of OpenSSL that is currently supported.

**See Also**

https://www.openssl.org/policies/releasestrat.html
http://www.nessus.org/u?4d55548d

**Output**

```
    Installed version  : 0.9.6b
    Supported versions : 1.1.0 / 1.0.2
    EOL URL            : https://www.openssl.org/policies/releasestrat.html
```

| Port | Hosts |
|---|---|
| 443 / tcp / www | 192.168.43.163 |
| 80 / tcp / www | 192.168.43.163 |

**Plugin Details**

| | |
|---|---|
| Severity: | Critical |
| ID: | 78555 |
| Version: | 1.9 |
| Type: | remote |
| Family: | Web Servers |
| Published: | October 17, 2014 |
| Modified: | September 22, 2020 |

**Risk Information**

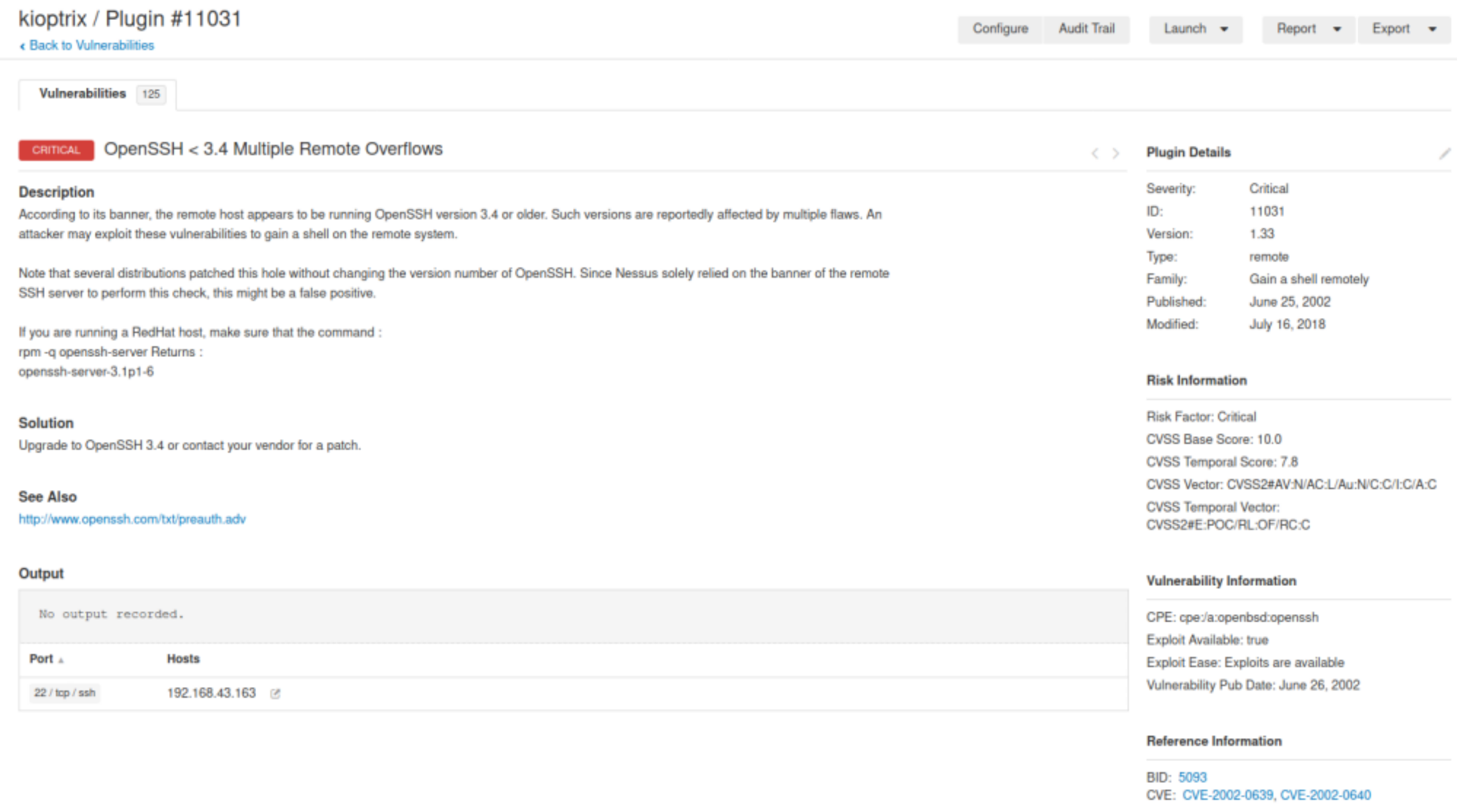
Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

CPE: cpe:/a:openssl:openssl
Unsupported by vendor: true

**Reference Information**

IAVA: 0001-A-0572



## kioptrix / Plugin #11031

### OpenSSH < 3.4 Multiple Remote Overflows

**Description**

According to its banner, the remote host appears to be running OpenSSH version 3.4 or older. Such versions are reportedly affected by multiple flaws. An attacker may exploit these vulnerabilities to gain a shell on the remote system.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :
rpm -q openssh-server Returns :
openssh-server-3.1p1-6

**Solution**

Upgrade to OpenSSH 3.4 or contact your vendor for a patch.

**See Also**

http://www.openssh.com/txt/preauth.adv

**Output**

```
No output recorded.
```

| Port | Hosts |
|---|---|
| 22 / tcp / ssh | 192.168.43.163 |

**Plugin Details**

| | |
|---|---|
| Severity: | Critical |
| ID: | 11031 |
| Version: | 1.33 |
| Type: | remote |
| Family: | Gain a shell remotely |
| Published: | June 25, 2002 |
| Modified: | July 16, 2018 |

**Risk Information**

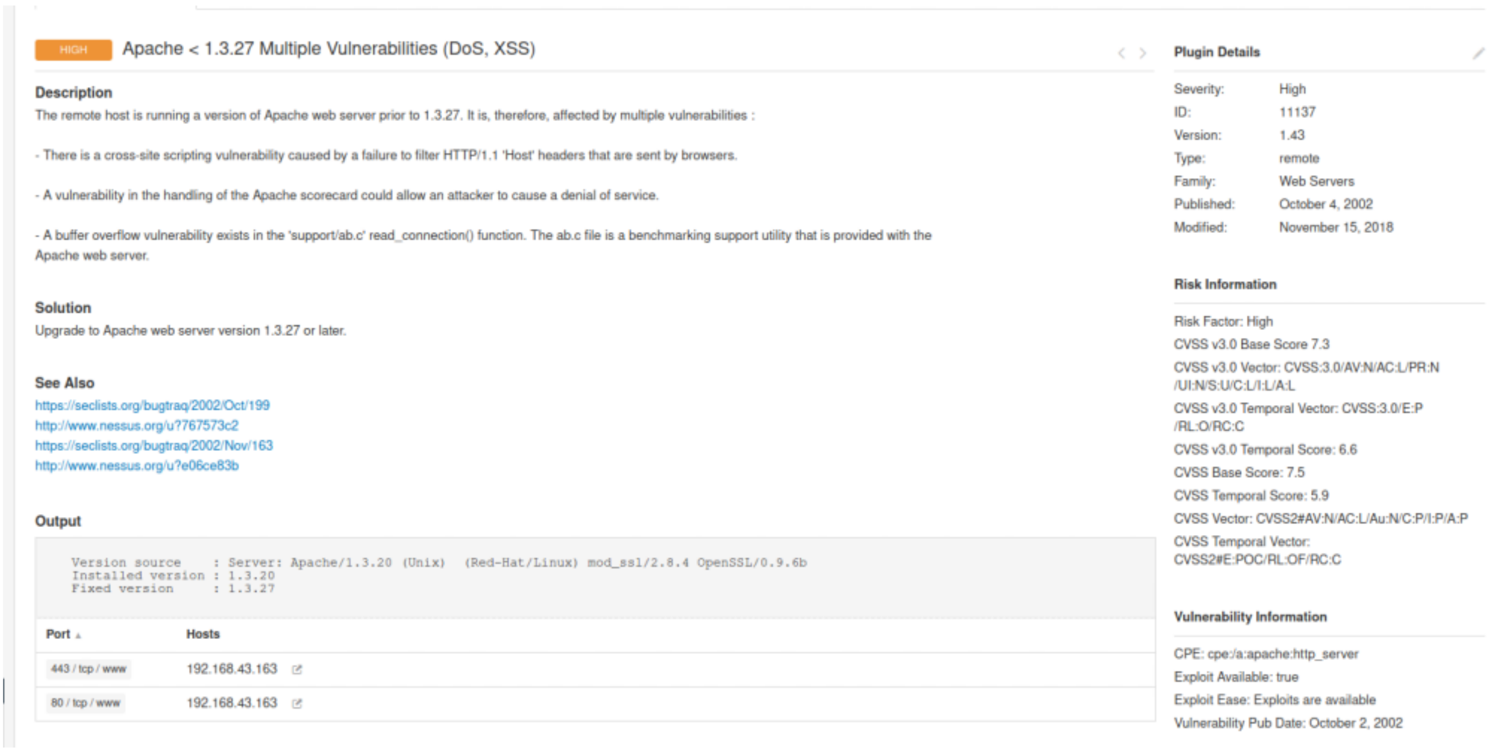
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 7.8
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

**Vulnerability Information**

CPE: cpe:/a:openbsd:openssh
Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: June 26, 2002

**Reference Information**

BID: 5093
CVE: CVE-2002-0639, CVE-2002-0640



### Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)

**Description**

The remote host is running a version of Apache web server prior to 1.3.27. It is, therefore, affected by multiple vulnerabilities :

- There is a cross-site scripting vulnerability caused by a failure to filter HTTP/1.1 'Host' headers that are sent by browsers.

- A vulnerability in the handling of the Apache scorecard could allow an attacker to cause a denial of service.

- A buffer overflow vulnerability exists in the 'support/ab.c' read_connection() function. The ab.c file is a benchmarking support utility that is provided with the Apache web server.

**Solution**

Upgrade to Apache web server version 1.3.27 or later.

**See Also**

https://seclists.org/bugtraq/2002/Oct/199
http://www.nessus.org/u?767573c2
https://seclists.org/bugtraq/2002/Nov/163
http://www.nessus.org/u?e06ce83b

**Output**

```
  Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
  Installed version : 1.3.20
  Fixed version     : 1.3.27
```

| Port | Hosts |
|---|---|
| 443 / tcp / www | 192.168.43.163 |
| 80 / tcp / www | 192.168.43.163 |

**Plugin Details**

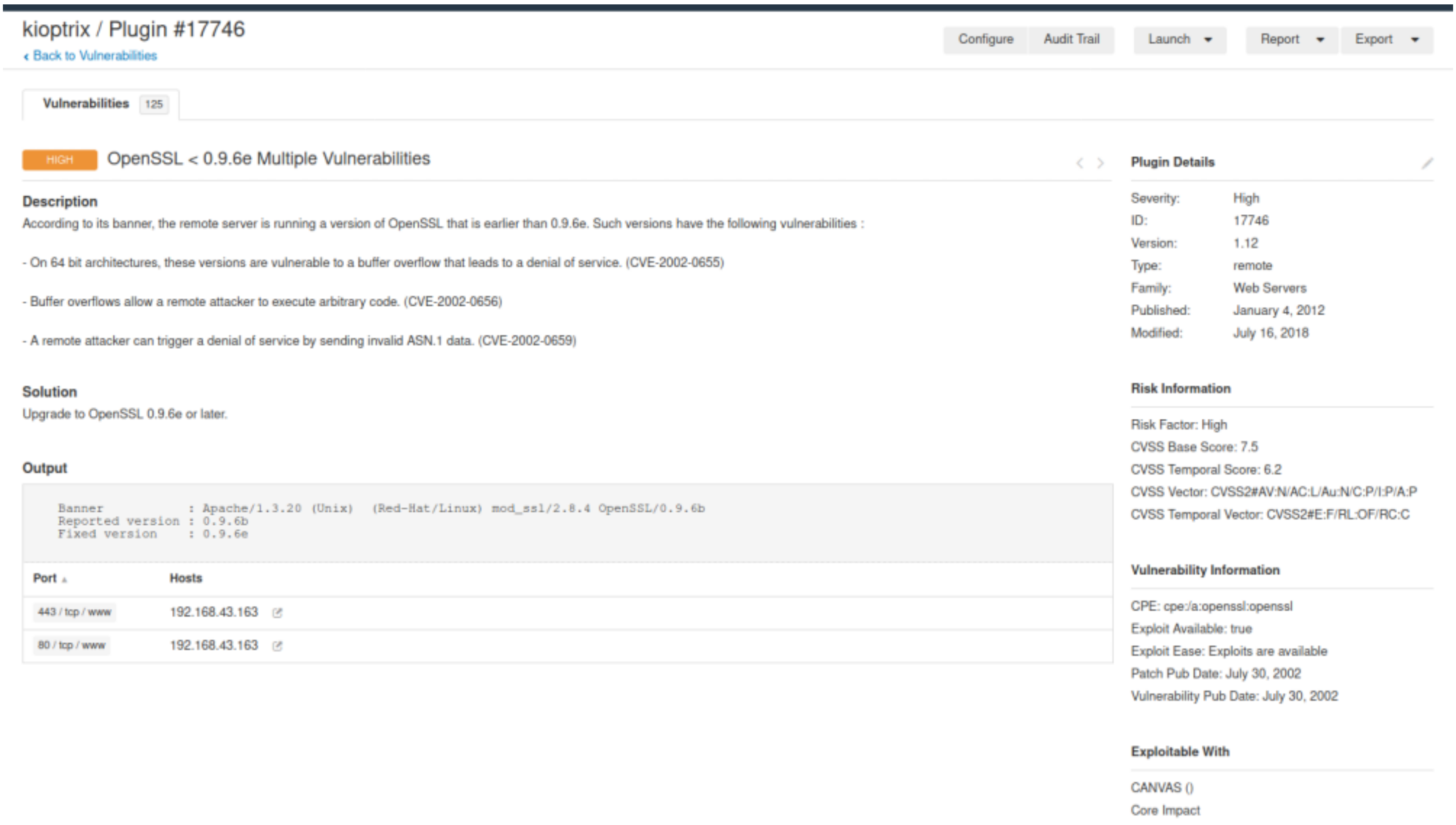
| | |
|---|---|
| Severity: | High |
| ID: | 11137 |
| Version: | 1.43 |
| Type: | remote |
| Family: | Web Servers |
| Published: | October 4, 2002 |
| Modified: | November 15, 2018 |

**Risk Information**

Risk Factor: High
CVSS v3.0 Base Score 7.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C
CVSS v3.0 Temporal Score: 6.6
CVSS Base Score: 7.5
CVSS Temporal Score: 5.9
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

**Vulnerability Information**

CPE: cpe:/a:apache:http_server
Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: October 2, 2002



## kioptrix / Plugin #17746

‹ Back to Vulnerabilities

Vulnerabilities 125

HIGH OpenSSL < 0.9.6e Multiple Vulnerabilities

### Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6e. Such versions have the following vulnerabilities :

- On 64 bit architectures, these versions are vulnerable to a buffer overflow that leads to a denial of service. (CVE-2002-0655)

- Buffer overflows allow a remote attacker to execute arbitrary code. (CVE-2002-0656)

- A remote attacker can trigger a denial of service by sending invalid ASN.1 data. (CVE-2002-0659)

### Solution

Upgrade to OpenSSL 0.9.6e or later.

### Output

```
   Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
   Reported version : 0.9.6b
   Fixed version    : 0.9.6e
```

| Port ▲ | Hosts |
|---|---|
| 443 / tcp / www | 192.168.43.163 |
| 80 / tcp / www | 192.168.43.163 |

### Plugin Details

| | |
|---|---|
| Severity: | High |
| ID: | 17746 |
| Version: | 1.12 |
| Type: | remote |
| Family: | Web Servers |
| Published: | January 4, 2012 |
| Modified: | July 16, 2018 |

### Risk Information

Risk Factor: High

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

### Vulnerability Information

CPE: cpe:/a:openssl:openssl

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: July 30, 2002

Vulnerability Pub Date: July 30, 2002

### Exploitable With

CANVAS ()

Core Impact