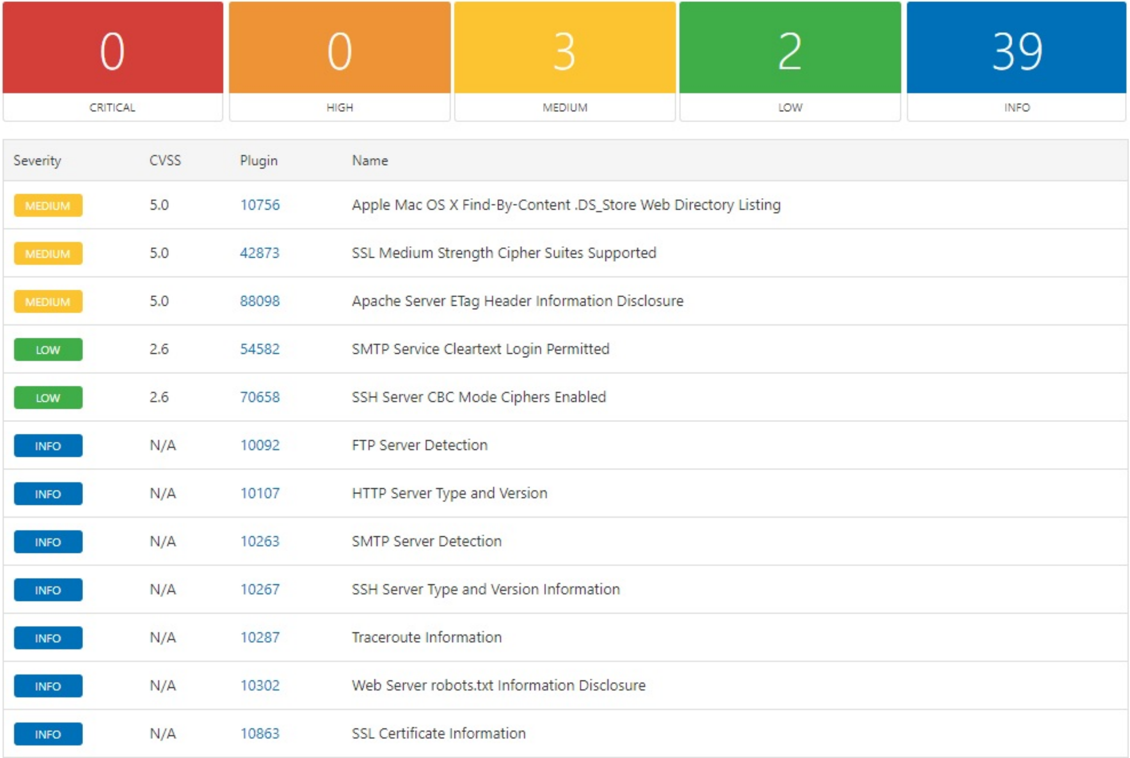
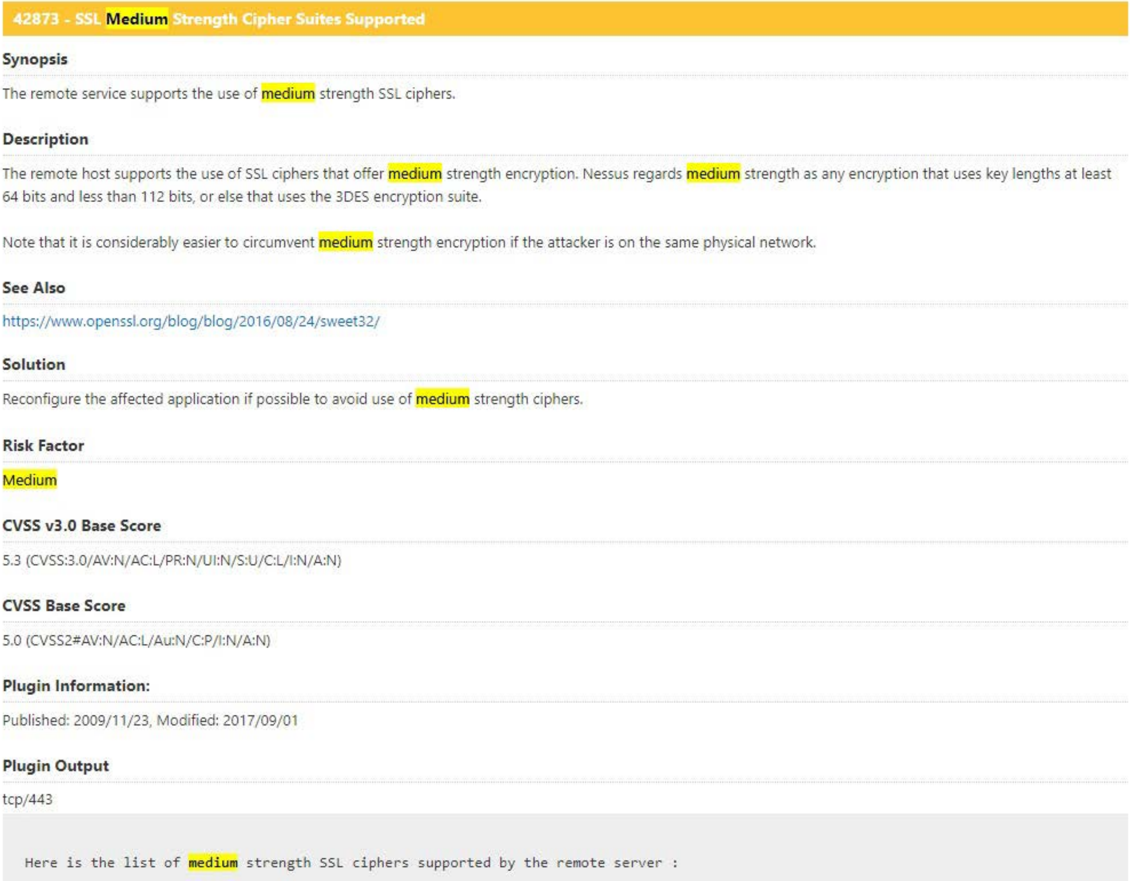


0	0	3	2	39
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
MEDIUM	5.0	10756	Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	5.0	88098	Apache Server ETag Header Information Disclosure
LOW	2.6	54582	SMTP Service Cleartext Login Permitted
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10302	Web Server robots.txt Information Disclosure
INFO	N/A	10863	SSL Certificate Information



42873 - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/443

```

  Here is the list of medium strength SSL ciphers supported by the remote server :
```