



MCUXpresso Web SDK builder advanced scan

Report generated by Nessus™

Wed, 23 Mar 2022 14:17:14 CDT

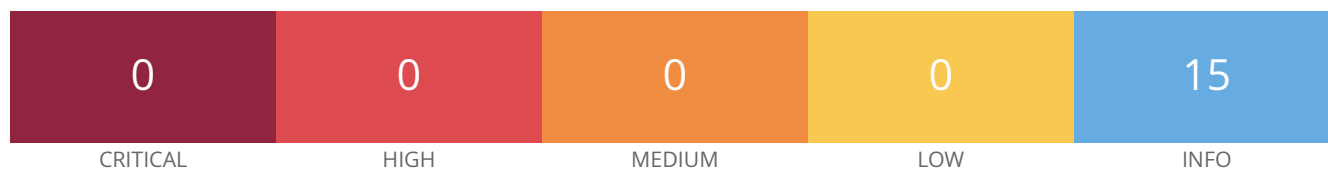
TABLE OF CONTENTS

Vulnerabilities by Host

• mcuxpresso.nxp.com.....	4
---------------------------	---

Vulnerabilities by Host

mcuxpresso.nxp.com



Scan Information

Start time: Wed Mar 23 13:46:24 2022

End time: Wed Mar 23 14:17:14 2022

Host Information

DNS Name: mcuxpresso.nxp.com

IP: 23.37.33.215

OS: AIX 5.3

Vulnerabilities

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF

IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
URL      : http://mcuxpresso.nxp.com/  
Version  : unknown  
backported : 0
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2022/02/14

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :
```

```
cpe:/o:ibm:aix:5.3 -> IBM AIX
```

```
Following application CPE matched on the remote system :
```

```
cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 65
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

<http://www.nessus.org/u?d9c03a9a>

<http://www.nessus.org/u?b019cbdb>

[https://www.owasp.org/index.php/Test_HTTP_Methods_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/80/www

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST PUT are allowed on :

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :  
Apache
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
23.37.33.215 resolves as a23-37-33-215.deploy.static.akamaitechnologies.com.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 302 Moved Temporarily

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: Apache

Location: https://mcuxpresso.nxp.com/

Content-Length: 211

Content-Type: text/html; charset=iso-8859-1

Cache-Control: max-age=0

Expires: Wed, 23 Mar 2022 19:12:53 GMT

Date: Wed, 23 Mar 2022 19:12:53 GMT

Connection: keep-alive

Server-Timing: cdn-cache; desc=MISS

Server-Timing: edge; dur=99

Server-Timing: origin; dur=49

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>302 Found</title>

</head><body>

<h1>Found</h1>

```
<p>The document has moved <a href="https://mcuxpresso.nxp.com/">here</a>.</p>
</body></html>
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
Request      : http://mcuxpresso.nxp.com/
HTTP response : HTTP/1.1 302 Moved Temporarily
Redirect to   : https://mcuxpresso.nxp.com/
Redirect type  : 30x redirect
```

Note that Nessus did not receive a 200 OK response from the last examined redirect.

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```


19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.1.1
Nessus build : X20061
Plugin feed version : 202203221746
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : MCUXpresso Web SDK builder advanced scan
```

```
Scan policy used : MCUXpresso Web SDK builder advanced scan
Scanner IP : 10.0.2.15

WARNING : No port scanner was enabled during the scan. This may
lead to incomplete results.

Port range : default
Ping RTT : 46.745 ms
Thorough tests : yes
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2022/3/23 13:46 CDT
Scan duration : 1840 sec
```

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : AIX 5.3  
Confidence level : 65  
Method : SinFP
```

```
The remote host is running AIX 5.3
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.2.15 to 23.37.33.215 :  
10.0.2.15  
10.0.2.2  
23.37.33.215  
  
Hop Count: 2
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :
```

```
http://mcuxpresso.nxp.com/vT_nuFJxdjPS.html
```