

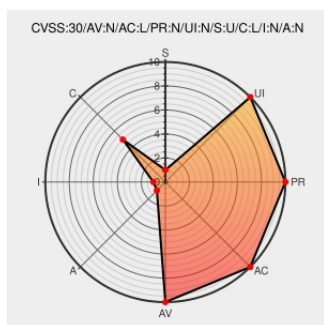


CVE-2016-1378

Published on: 04/13/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

CVE-2016-1378

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of **ios** from **Cisco** contain the following vulnerability:

Cisco IOS before 15.2(2)E1 on Catalyst switches allows remote attackers to obtain potentially sensitive software-version information via a request to the Network Mobility Services Protocol (NMSP) port, aka Bug ID CSCum62591.

CVE-2016-1378 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Cisco Catalyst Switches Network Mobility Services Protocol Port Information Disclosure Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20160413 Cisco Catalyst Switches Network Mobility Services Protocol Port Information Disclosure Vulnerability
Cisco Catalyst Switch NMSP Port Lets Remote Users Obtain	www.securitytracker.com	SECTrack 1035566

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	15.1(1)sg	All	All	All
Operating System	Cisco	ios	15.1(1)sg1	All	All	All
Operating System	Cisco	ios	15.1(1)sg2	All	All	All
Operating System	Cisco	ios	15.1(1)sy	All	All	All
Operating System	Cisco	ios	15.1(1)sy1	All	All	All
Operating System	Cisco	ios	15.1(1)sy2	All	All	All
Operating System	Cisco	ios	15.1(1)sy3	All	All	All
Operating System	Cisco	ios	15.1(1)sy4	All	All	All
Operating System	Cisco	ios	15.1(1)sy5	All	All	All
Operating System	Cisco	ios	15.1(1)sy6	All	All	All
Operating System	Cisco	ios	15.1(2)sg	All	All	All
Operating System	Cisco	ios	15.1(2)sg1	All	All	All
Operating System	Cisco	ios	15.1(2)sg2	All	All	All
Operating System	Cisco	ios	15.1(2)sg3	All	All	All
Operating System	Cisco	ios	15.1(2)sg4	All	All	All
Operating System	Cisco	ios	15.1(2)sg5	All	All	All
Operating System	Cisco	ios	15.1(2)sg6	All	All	All

Operating System	Cisco	los	15.1(2)sg7	All	All	All
Operating System	Cisco	los	15.1(2)sy	All	All	All
Operating System	Cisco	los	15.1(2)sy1	All	All	All
Operating System	Cisco	los	15.1(2)sy2	All	All	All
Operating System	Cisco	los	15.1(2)sy3	All	All	All
Operating System	Cisco	los	15.1(2)sy4	All	All	All
Operating System	Cisco	los	15.1(2)sy4a	All	All	All
Operating System	Cisco	los	15.1(2)sy5	All	All	All
Operating System	Cisco	los	15.1(2)sy6	All	All	All
Operating System	Cisco	los	15.1(2)sy7	All	All	All
Operating System	Cisco	los	15.1(2)sy8	All	All	All
Operating System	Cisco	los	15.1\1\sg	All	All	All
Operating System	Cisco	los	15.1\1\sg1	All	All	All
Operating System	Cisco	los	15.1\1\sg2	All	All	All
Operating System	Cisco	los	15.1\1\sy	All	All	All
Operating System	Cisco	los	15.1\1\sy1	All	All	All
Operating System	Cisco	los	15.1\1\sy2	All	All	All
Operating System	Cisco	los	15.1\1\sy3	All	All	All
Operating System	Cisco	los	15.1\1\sy4	All	All	All
Operating System	Cisco	los	15.1\1\sy5	All	All	All
Operating System	Cisco	los	15.1\1\sy6	All	All	All
Operating System	Cisco	los	15.1\2\sg	All	All	All
Operating System	Cisco	los	15.1\2\sg1	All	All	All

Operating System	Cisco	los	15.1\2\sg2	All	All	All
Operating System	Cisco	los	15.1\2\sg3	All	All	All
Operating System	Cisco	los	15.1\2\sg4	All	All	All
Operating System	Cisco	los	15.1\2\sg5	All	All	All
Operating System	Cisco	los	15.1\2\sg6	All	All	All
Operating System	Cisco	los	15.1\2\sg7	All	All	All
Operating System	Cisco	los	15.1\2\sy	All	All	All
Operating System	Cisco	los	15.1\2\sy1	All	All	All
Operating System	Cisco	los	15.1\2\sy2	All	All	All
Operating System	Cisco	los	15.1\2\sy3	All	All	All
Operating System	Cisco	los	15.1\2\sy4	All	All	All
Operating System	Cisco	los	15.1\2\sy4a	All	All	All
Operating System	Cisco	los	15.1\2\sy5	All	All	All
Operating System	Cisco	los	15.1\2\sy6	All	All	All
Operating System	Cisco	los	15.1\2\sy7	All	All	All
Operating System	Cisco	los	15.1\2\sy8	All	All	All
Operating System	Cisco	los	15.1\1\sg	All	All	All
Operating System	Cisco	los	15.1\1\sg1	All	All	All
Operating System	Cisco	los	15.1\1\sg2	All	All	All
Operating System	Cisco	los	15.1\1\sy	All	All	All
Operating System	Cisco	los	15.1\1\sy1	All	All	All
Operating System	Cisco	los	15.1\1\sy2	All	All	All
Operating System	Cisco	los	15.1\1\sy3	All	All	All

Operating System	Cisco	ios	15.1\ (1\)sy4	All	All	All
Operating System	Cisco	ios	15.1\ (1\)sy5	All	All	All
Operating System	Cisco	ios	15.1\ (1\)sy6	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg1	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg2	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg3	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg4	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg5	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg6	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sg7	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy1	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy2	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy3	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy4	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy4a	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy5	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy6	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy7	All	All	All
Operating System	Cisco	ios	15.1\ (2\)sy8	All	All	All
cpe:2.3:o:cisco:ios:15.1(1)sg:*****:						
cpe:2.3:o:cisco:ios:15.1(1)sg1:*****:						

cpe:2.3:o:cisco:ios:15.1(1)sg2:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy1:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy2:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy3:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy4:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy5:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy6:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg1:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg2:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg3:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg4:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg5:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg6:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg7:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy1:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy2:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy3:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy4:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy4a:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy5:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy6:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy7:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy8:*****:
cpe:2.3:o:cisco:ios:15.1(1)sg:*****:
cpe:2.3:o:cisco:ios:15.1(1)sg1:*****:
cpe:2.3:o:cisco:ios:15.1(1)sg2:*****:

```
cpe:2.3:o:cisco:ios:15.1(1)sy:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1(1)sy1:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.1(1)sy2:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1(1)sy3:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.1(1)sy4:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:cisco:ios:15.1(1)sy5:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1\:(1\)sy6:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1(2)sg:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sg1:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sg2:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sg3:::~
```

cpe:2.3:o:cisco:ios:15.1\((2\)sg4:::~

```
cpe:2.3:o:cisco:ios:15.1\((2\)sg5:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sg6:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sg7:::~
```

```
cpe:2.3:o:cisco:ios:15.1(2)sy:~::~::~:
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy1:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy2:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy3:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy4:::~
```

```
cpe:2.3:o:cisco:ios:15.1(2)sy4a:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy5:::~::~:
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy6:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy7:::~
```

```
cpe:2.3:o:cisco:ios:15.1\((2\)sy8:::~
```

```
cpe:2.3:o:cisco:ios:15.1(1)sg:::*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1\((1\)sg1:::~
```

```
cpe:2.3:o:cisco:ios:15.1\:(1\):sg2:*:*:*:*:*:
```

cpe:2.3:o:cisco:ios:15.1(1)sy:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy1:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy2:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy3:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy4:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy5:*****:
cpe:2.3:o:cisco:ios:15.1(1)sy6:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg1:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg2:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg3:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg4:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg5:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg6:*****:
cpe:2.3:o:cisco:ios:15.1(2)sg7:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy1:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy2:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy3:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy4:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy4a:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy5:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy6:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy7:*****:
cpe:2.3:o:cisco:ios:15.1(2)sy8:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)