

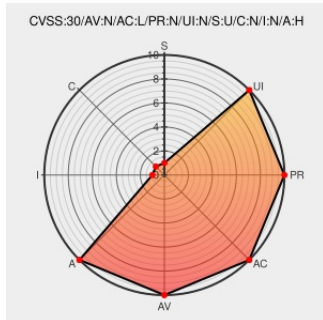


CVE-2017-6657

Published on: 05/16/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6657

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

Certain versions of [Snort](#) from [Cisco](#) contain the following vulnerability:

Cisco Sourcefire Snort 3.0 before build 233 mishandles Ether Type Validation. Since valid ether type and IP protocol numbers do not overlap, Snort++ stores all protocol decoders in a single array. That makes it possible to craft packets that have IP protocol numbers in the ether type field which will confuse the Snort++ decoder. For example, an eth:llc:snap:icmp6 packet will cause a crash because there is no ip6

header with which to calculate the icmp6 checksum. Affected decoders include gre, llc, trans_bridge, cisco metadata, linux_sll, and token_ring. The fix adds a check in the packet manager to validate the ether type before indexing the decoder array. An out of range ether type will raise 116:473.

CVE-2017-6657 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description

Cisco Snort++ Protocol Decoder Denial of Service Vulnerabilities

Tags

Vendor Advisory

tools.cisco.com

text/html

Link

MISC

tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170515-snort

Description

Cisco Snort++ Protocol Decoder Bugs Let Remote Users Deny Service - SecurityTracker

Tags

www.securitytracker.com

text/html

Link

SECTrack 1038483

Description

Snort Blog: Snort++ Vulnerabilities Found

Tags

Third Party Advisory

web.archive.org

text/html

Inactive Link

Not Archived

Link

CONFIRM

blog.snort.org/2017/05/snort-vulnerabilities-found.html

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
Application	Cisco	Snort	-	All	All	All
Application	Cisco	Snort	-	All	All	All
Application	Cisco	Snort	-	All	All	All

cpe:2.3:a:cisco:snort+-:~::~::~:

cpe:2.3:a:cisco:snort\+\:~::~::~:

cpe:2.3:a:cisco:snort\+\:~::~::~:

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](#)