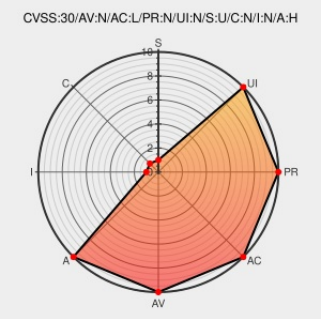
CVE-2017-6657

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, ciscometadata, 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	Tags	Link
Cisco Snort++ Protocol Decoder Denial of Service Vulnerabilities	Vendor Advisory tools.cisco.com text/html	MISC tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170515-snort
Cisco Snort++ Protocol Decoder Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1038483
Snort Blog: Snort++ Vulnerabilities Found	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM blog.snort.org/2017/05/snort-vulnerabilities-found.html

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→