

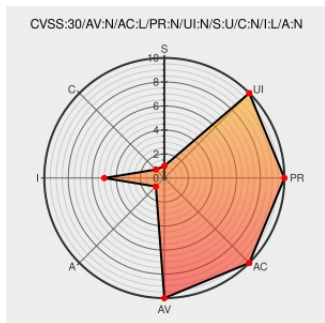


CVE-2016-10728

Published on: 07/23/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:00 PM UTC

CVE-2016-10728

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

Certain versions of [Suricata](#) from [Suricata-ids](#) contain the following vulnerability:

An issue was discovered in Suricata before 3.1.2. If an ICMPv4 error packet is received as the first packet on a flow in the to_client direction, it confuses the rule grouping lookup logic. The toclient inspection will then continue with the wrong rule group. This can lead to missed detection.

CVE-2016-10728 has been assigned by [M](#) cve@mitre.org 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	NONE	LOW	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Suricata 3.1.2 released! Suricata	Vendor Advisory suricata-ids.org text/html	MISC suricata-ids.org/2016/09/07/suricata-3-1-2-released/

GitHub - kirillwow/ids_bypass: IDS Bypass tricks

Exploit

Third Party Advisory

github.com

text/html

 MISC github.com/kirillwow/ids_bypass

Bug #1880: icmpv4 error packets can lead to missed detection in tcp/udp - Suricata - Open Information Security Foundation

Third Party Advisory

redmine.openinfosecfoundation.org

text/html

 MISC redmine.openinfosecfoundation.org/issues/1880

[SECURITY] [DLA 1508-1] suricata security update

Third Party Advisory

lists.debian.org

text/html

 MLIST [\[debian-lts-announce\] 20180919 \[SECURITY\] \[DLA 1508-1\] suricata security update](#)

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	Suricata-ids	Suricata	All	All	All	All
Application	Suricata-ids	Suricata	All	All	All	All

cpe:2.3:a:suricata-ids:suricata:*****:

cpe:2.3:a:suricata-ids:suricata:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)