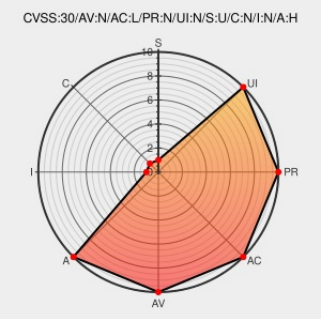
CVE-2018-12680

Published on: 04/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:24 PM UTC

CVE-2018-12680

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Coapthon from Coapthon Project contain the following vulnerability:

The Serialize.deserialize() method in CoAPthon 3.1, 4.0.0, 4.0.1, and 4.0.2 mishandles certain exceptions, leading to a denial of service in applications that use this library (e.g., the standard CoAP server, CoAP client, CoAP reverse proxy, example collect CoAP server and client) when they receive crafted CoAP messages.

CVE-2018-12680 has been assigned by cve@mitre.org 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
Denial of Service vulnerability caused by improper exception handling while parsing of CoAP messages · Issue #135 · Tanganelli/CoAPthon · GitHub	Exploit, Issue Tracking, Third Party Advisory	MISC github.com/Tanganelli/CoAPthon/issues/135

github.com
text/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.

Related QID Numbers

981282 Python (pip) Security Update for CoAPthon (GHSA-5xc6-fpc7-4qvg)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coapthon Project	Coapthon	3.1	All	All	All
Application	Coapthon Project	Coapthon	4.0.0	All	All	All
Application	Coapthon Project	Coapthon	4.0.1	All	All	All
Application	Coapthon Project	Coapthon	4.0.2	All	All	All
Application	Coapthon Project	Coapthon	3.1	All	All	All
Application	Coapthon Project	Coapthon	4.0.0	All	All	All
Application	Coapthon Project	Coapthon	4.0.1	All	All	All
Application	Coapthon Project	Coapthon	4.0.2	All	All	All

cpe:2.3:a:coapthon_project:coapthon:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:coapthon_project:coapthon:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:coapthon_project:coapthon:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:coapthon_project:coapthon:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:coapthon_project:coapthon:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:coapthon_project:coapthon:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:coapthon_project:coapthon:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:coapthon_project:coapthon:4.0.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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