

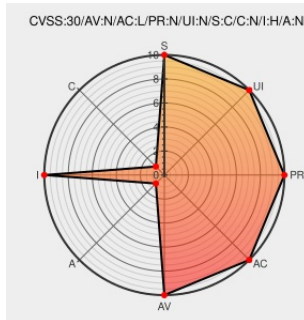


CVE-2018-3911

Published on: 08/23/2018 12:00:00 AM UTC

Last Modified on: 02/04/2023 01:23:00 AM UTC

CVE-2018-3911

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

Certain versions of [Sth-eth-250](#) from [Samsung](#) contain the following vulnerability:

An exploitable HTTP header injection vulnerability exists in the remote servers of Samsung SmartThings Hub STH-ETH-250 - Firmware version 0.20.17. The hubCore process listens on port 39500 and relays any unauthenticated message to SmartThings' remote servers, which insecurely handle JSON messages, leading to partially controlled requests generated toward the internal video-core process. An attacker can send an HTTP request to trigger this vulnerability.

CVE-2018-3911 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Samsung](#) - **Samsung** version **Samsung SmartThings Hub STH-ETH-250 - Firmware version 0.20.17**

CVSS3 Score: **8.6 - HIGH**

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

TALOS-2018-0578 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

Tags

Exploit

Third Party Advisory

talosintelligence.com

text/html

Link

MISC

talosintelligence.com/vulnerability_reports/TALOS-2018-0578

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
Hardware	Samsung	Sth-eth-250	-	All	All	All
Hardware	Samsung	Sth-eth-250	-	All	All	All
Operating System	Samsung	Sth-eth-250 Firmware	0.20.17	All	All	All
Operating System	Samsung	Sth-eth-250 Firmware	0.20.17	All	All	All
cpe:2.3:h:samsung:sth-eth-250:-:*:*:*:*:*:						
cpe:2.3:h:samsung:sth-eth-250:-:*:*:*:*:*:						
cpe:2.3:o:samsung:sth-eth-250_firmware:0.20.17:*:*:*:*:*:						
cpe:2.3:o:samsung:sth-eth-250_firmware:0.20.17:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →