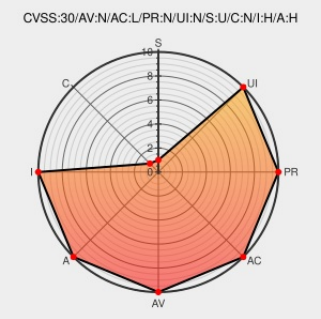
CVE-2018-3908

Published on: 08/28/2018 12:00:00 AM UTC

Last Modified on: 02/04/2023 01:24:00 AM UTC

CVE-2018-3908

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



Certain versions of Sth-eth-250 from Samsung contain the following vulnerability:

An exploitable vulnerability exists in the REST parser of video-core's HTTP server of the Samsung SmartThings Hub STH-ETH-250-Firmware version 0.20.17. The video-core process incorrectly handles pipelined HTTP requests, which allows successive requests to overwrite the previously parsed HTTP method, URL and body. With the implementation of the on_body callback, defined by sub_41734, an attacker can send an HTTP request to trigger this vulnerability.

CVE-2018-3908 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: 7.5 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
TALOS-2018-0577 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2018-0577

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→