

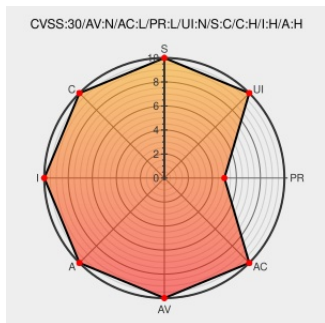


CVE-2018-3897

Published on: 09/10/2018 12:00:00 AM UTC

Last Modified on: 12/02/2022 10:59:00 PM UTC

CVE-2018-3897

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

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

An exploitable buffer overflow vulnerabilities exist in the `/cameras/XXXX/clips` handler of video-core's HTTP server of Samsung SmartThings Hub with Firmware version 0.20.17. The video-core process incorrectly extracts fields from a user-controlled JSON payload, leading to a buffer overflow on the stack. The `strncpy` call overflows the destination buffer, which has a size of 52 bytes. An attacker can send an arbitrarily long "callbackUrl" value in order to exploit this vulnerability.

CVE-2018-3897 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

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

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description

TALOS-2018-0570 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

Tags

Exploit

Third Party Advisory

talosintelligence.com

text/html

Link

MISC

talosintelligence.com/vulnerability_reports/TALOS-2018-0570

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 →