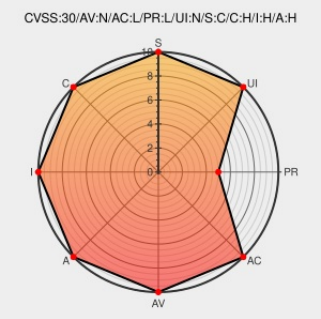
CVE-2018-3896

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

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

CVE-2018-3896

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 "correlationId" value in order to exploit this vulnerability.

CVE-2018-3896 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	Tags	Link
TALOS-2018-0570 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2018-0570

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→