CVE-2018-3912

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

Last Modified on: 02/17/2023 03:43:00 AM UTC

CVE-2018-3912

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

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

On Samsung SmartThings Hub STH-ETH-250 devices with firmware version 0.20.17, the video-core process insecurely extracts the fields from the "shard" table of its SQLite database, leading to a buffer overflow on the stack. The strcpy call overflows the destination buffer, which has a size of 128 bytes. An attacker can send an arbitrarily long "secretKey" value in order to exploit this vulnerability.

CVE-2018-3912 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: 7.8 - HIGH

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

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

TALOS-2018-0581 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Third Party Advisory www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2018-0581

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

Social Mentions

Source	Title	Posted (UTC)
@fprado28	Que massa.. já vou atrás do orçamento para a próxima compra Vou poder testar os CVE-2018-3912 / CVE-2021-25508 / C… twitter.com/i/web/status/1…	2022-03-30 17:34:26

← Previous ID

Next ID→