



CVE-2018-6242

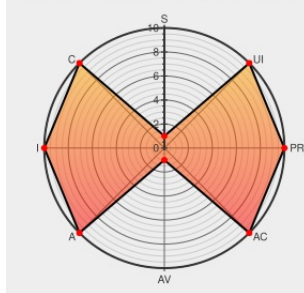
Published on: 05/01/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-6242

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

CVSS:30/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Tegra Bootrom Rcm](#) from [Nvidia](#) contain the following vulnerability:

Some NVIDIA Tegra mobile processors released prior to 2016 contain a buffer overflow vulnerability in BootROM Recovery Mode (RCM). An attacker with physical access to the device's USB and the ability to force the device to reboot into RCM could exploit the vulnerability to execute unverified code.

CVE-2018-6242 has been assigned by psirt@nvidia.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Nvidia Corporation** - **Some NVIDIA Tegra Mobile Processors** version n/a

CVSS3 Score: **6.8 - MEDIUM**

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

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Notice: NVIDIA Tegra RCM Vulnerability	Vendor Advisory	CONFIRM

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

Exploit/POC from Github

Rust implementation of the Fusée Gelée exploit (CVE-2018-6242) for Tegra processors.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nvidia	Tegra Bootrom Rcm	-	All	All	All
Application	Nvidia	Tegra Bootrom Rcm	-	All	All	All
Hardware 	Nvidia	Tegra Mobile Processor	-	All	All	All
Hardware 	Nvidia	Tegra Mobile Processor	-	All	All	All

```
cpe:2.3:a:nvidia:tegra_bootrom_rcm:-:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:nvidia:tegra_bootrom_rcm:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:nvidia:tegra_mobile_processor:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:nvidia:tegra mobile processor:-:*:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→