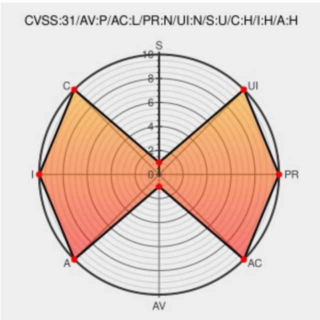
CVE-2019-18216

Published on: 10/20/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-18216

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



Certain versions of Rog Zephyrus M Gm501gs from Asus contain the following vulnerability:

** DISPUTED ** The BIOS configuration design on ASUS ROG Zephyrus M GM501GS laptops with BIOS 313 relies on the main battery instead of using a CMOS battery, which reduces the value of a protection mechanism in which booting from a USB device is prohibited. Attackers who have physical laptop access can exhaust the main battery to reset the BIOS configuration, and then achieve direct access to the hard drive by booting a live USB OS without disassembling the laptop. NOTE: the vendor has apparently indicated that this is "normal" and use of the same battery for the BIOS and the overall system is a "new design." However, the vendor apparently plans to "improve" this an unspecified later time.

CVE-2019-18216 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

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
ASUS ROG BIOS Reset on Lost Battery Power - Blog Teknis modpr0be	Third Party Advisory blog.modpr0.be text/html	MISC blog.modpr0.be/2019/10/18/asus-rog-bios-reset-on-lost-battery-power/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Asus	Rog Zephyrus M Gm501gs	-	All	All	All
Hardware	Asus	Rog Zephyrus M Gm501gs	-	All	All	All
Operating System	Asus	Rog Zephyrus M Gm501gs Firmware	-	All	All	All
Operating System	Asus	Rog Zephyrus M Gm501gs Firmware	-	All	All	All

cpe:2.3:h:asus:rog_zephyrus_m_gm501gs:-:*:*:*:*:*:*:*:

cpe:2.3:h:asus:rog_zephyrus_m_gm501gs:-:*:*:*:*:*:*:*:

cpe:2.3:o:asus:rog_zephyrus_m_gm501gs_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:asus:rog_zephyrus_m_gm501gs_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→