



CVE-2019-18216

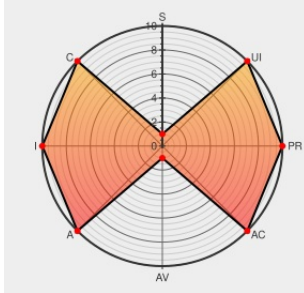
Published on: 10/20/2019 12:00:00 AM UTC

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

CVE-2019-18216

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

CVSS:31/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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 [M](#) 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.modpr0be text/html	 MISC blog.modpr0.be/2019/10/18/asus-rog-bios-reset-on-lost-battery-power/

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 🖨️🔗	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→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report