



CVE-2022-40246

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-40246
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-20 18:15:00 UTC
Updated	2022-09-26 14:22:00 UTC
Description	A potential attacker can write one byte by arbitrary address at the time of the PEI phase (only during S3 resume boot mode

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Intel	Nuc M15 Laptop Kit Lapbc510	-	All	All	All
Operating System	Intel	Nuc M15 Laptop Kit Lapbc510 Firmware	0072	All	All	All
Hardware	Intel	Nuc M15 Laptop Kit Lapbc710	-	All	All	All
Operating System	Intel	Nuc M15 Laptop Kit Lapbc710 Firmware	0072	All	All	All

References

Reference	Source	Link
[BRLY-2022-014] Arbitrary write vulnerability in PEI module leads to arbitrary code execution during PEI phase.	MISC	www.binarly.io
AMI Firmware Security Team	MISC	www.ami.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Binarly efiXplorer team

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)