



CVE-2021-41840

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

Summary

CVE	CVE-2021-41840
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-03 02:15:00 UTC
Updated	2022-03-29 16:36:00 UTC
Description	An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout tr

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Insyde	Insydeh2o	All	All	All	All

References

Reference	Source	Link	Tags
Insyde's Security Pledge Insyde Software	MISC	www.insyde.com	
cert-portal.siemens.com/productcert/pdf/ssa-306654.pdf	CONFIRM	cert-portal.siemens.com	
CVE-2021-41840 InsydeH2O Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Insyde Security Advisory 2022018 Insyde Software	MISC	www.insyde.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

590981 Siemens Industrial Products Insyde BIOS Multiple Vulnerabilities (SSA-306654)

© [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](#).

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