CVE-2021-31400

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-31400
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-19 11:15:00 UTC
Updated	2021-08-26 17:17:00 UTC
Description	An issue was discovered in tcp_pulloutofband() in tcp_in.c in HCC embedded InterNiche 4.0.1. The TCP out-of-band urgen

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hcc-embedded	Nichestack	All	All	All	All

References

Reference	Source	Link
New Critical Operational Technology Vulnerabilities Found on NicheStack – Mitigation Advised - Forescout	MISC	www.forescout.com
VU#608209 - NicheStack embedded TCP/IP has vulnerabilities	CERT-VN	www.kb.cert.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

590785 Schneider Electric Lexium ILE ILA ILS and Altivar Multiple Vulnerabilities (SEVD-2021-217-01)

591068 Rockwell Automation Products INFRA:HALT Interniche Multiple Vulnerabilities (PN1575)

© 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 registred 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