CVE-2020-35684

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

Summary

CVE	CVE-2020-35684
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-19 12:15:00 UTC
Updated	2021-08-26 18:21:00 UTC
Description	An issue was discovered in HCC Nichestack 3.0. The code that parses TCP packets relies on an unchecked value of the IP

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hcc-embedded	Nichestack	3.0	All	All	All
Hardware	Siemens	Sentron 3wa Com190	-	All	All	All
Operating System	Siemens	Sentron 3wa Com190 Firmware	All	All	All	All
Hardware	Siemens	Sentron 3wl Com35	-	All	All	All
Operating System	Siemens	Sentron 3wl Com35 Firmware	All	All	All	All

References

Reference	Source	Link
Home - Embedded Software and Systems	MISC	www.hcc-embedde
cert-portal.siemens.com/productcert/pdf/ssa-789208.pdf	CONFIRM	cert-portal.siemens
New Critical Operational Technology Vulnerabilities Found on NicheStack – Mitigation Advised - Forescout	MISC	www.forescout.con
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

590508 Siemens Interniche IP-Stack Multiple Vulnerabilities (SSA-789208)

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)

Free CVE JSON API cve.report/api

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