



CVE-2020-25066

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

Summary

CVE	CVE-2020-25066
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-22 22:15:00 UTC
Updated	2021-03-26 02:04:00 UTC
Description	A heap-based buffer overflow in the Treck HTTP Server component before 6.0.1.68 allows remote attackers to cause a der

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Treck	Tcp/ip	All	All	All	All
Application	Treck	Tcp/ip	All	All	All	All

References

Reference	Source	Link	Tags
January 2021 Treck TCP/IP Library Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Vulnerability Response Information - Treck Embedded TCP/IP Internet Protocols	CONFIRM	treck.com	Vendor
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

[590789](#) Schneider Electric Sepam ACE850 Treck Hypertext Transfer Protocol Server (HTTP Server) Vulnerability (SEVD-2021-012-03)

[590817](#) Schneider Electric Treck HTTP Server Vulnerability on TM3 Bus Coupler Modules Vulnerability (SEVD-2020-353-02)

© [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](#)