CVE-2020-12053

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-12053
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-22 20:15:00 UTC
Updated	2020-06-29 13:31:00 UTC
Description	In Unisys Stealth 3.4.x, 4.x and 5.x before 5.0.026, if certificate-based authorization is used without HTTPS, an endpoint co

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Unisys	Stealth	All	All	All	All
Application	Unisys	Stealth	All	All	All	All

References

Reference	Source	Link	Tags
Vulnerability Report - Endpoint Certificate Validation using HTTP may Erroneously Succeed	CONFIRM	public.support.unisys.com	Vend
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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

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