



CVE-2020-24620

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

Summary

CVE	CVE-2020-24620
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-01 17:15:00 UTC
Updated	2021-02-12 19:49:00 UTC
Description	Unisys Stealth(core) before 4.0.134 stores passwords in a recoverable format. Therefore, a search of Enterprise Manager c

Risk And Classification

Problem Types: CWE-798

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
Product Security Vulnerability Home	MISC	public.support.unisys.com	Vendor Adv
Vulnerability Report - Search of Enterprise Manager can potentially reveal credentials	CONFIRM	public.support.unisys.com	Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

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](#)