



# CVE-2021-28492

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-28492
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-20 16:15:00 UTC
<b>Updated</b>	2021-05-04 15:03:00 UTC
<b>Description</b>	Unisys Stealth (core) 5.x before 5.0.048.0, 5.1.x before 5.1.017.0, and 6.x before 6.0.037.0 stores passwords in a recoverable

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
Product Security Vulnerability Home	MISC	<a href="https://public.support.unisys.com">public.support.unisys.com</a>	
Vulnerability Report - Stealth Services Password Exposed	CONFIRM	<a href="https://public.support.unisys.com">public.support.unisys.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)**