

CVE-2021-44207

Acclaim Systems USAHERDS Use of Hard-Coded Credentials Vulnerability

CISA KEV since Dec 23, 2024

Actively exploited

Acclaim USAHERDS through 7.4.0.1 uses hard-coded credentials.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.1 High · NVD	EPSS 0.176 97.1st percentile · FIRST	CISA DEADLINE Jan 13, 2025 KEV since 2024 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.176 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Please contact the product developer for support and vulnerability mitigation.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
usaherds	≤ 7.4.0.1	after 7.4.0.1	NVD

Sources

Vendor guidance	acclaimsystems.com	acclaimsystems.com	acclaimsystems.com/#contact
tnatc.org	tnatc.org/#contact	NVD	nvd.nist.gov/vuln/detail/CVE-2021-44207
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-31057
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-44207		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.