

CVE-2023-45727

North Grid Proself Improper Restriction of XML External Entity (XXE) Reference Vulnerability

CISA KEV since Dec 3, 2024

Actively exploited

Proself Enterprise/Standard Edition Ver5.62 and earlier, Proself Gateway Edition Ver1.65 and earlier, and Proself Mail Sanitize Edition Ver1.08 and earlier allow a remote unauthenticated attacker to conduct XML External Entity (XXE) attacks. By processing a specially crafted request containing malformed XML data, arbitrary files on the server containing account information may be read by the attacker.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.048 91.9th percentile · FIRST	CISA DEADLINE Dec 24, 2024 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	0.048 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
proself	< 1.09 < 1.66 < 5.63	1.09 · 1.66 · 5.63	NVD

Sources

Vendor guidance github.com/advisories/GHSA-m745-jcvj-8cx6
NVD nvd.nist.gov/vuln/detail/CVE-2023-45727**Additional guidance** proself.jp/information/153/
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2023-45727**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2023-50016

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