



CVE-2023-39415

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

Summary

CVE	CVE-2023-39415
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-18 10:15:00 UTC
Updated	2023-08-23 16:48:00 UTC
Description	Improper authentication vulnerability in Proself Enterprise/Standard Edition Ver5.61 and earlier, Proself Gateway Edition Ver5.61 and earlier

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Northgrid	Proself	All	All	All	All
Application	Northgrid	Proself	All	All	All	All
Application	Northgrid	Proself	All	All	All	All
Application	Northgrid	Proself	All	All	All	All

References

Reference
お知らせ: [至急]Proselfのゼロディ脆弱性による攻撃発生について(更新) / オンラインストレージ構築パッケージ Proself (プロセルフ) / 株式会社北緯グリッド
JVN#19661362: Multiple vulnerabilities in Proself
お知らせ: Proselfのゼロディ脆弱性への対応バージョンに関する補足 / オンラインストレージ構築パッケージ Proself (プロセルフ) / 株式会社北緯グリッド
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)