



CVE-2022-1065

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

Summary

CVE	CVE-2022-1065
State	PUBLIC
Assigner	vulnerability@ncsc.ch
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-19 08:15:00 UTC
Updated	2022-04-27 14:56:00 UTC
Description	A vulnerability within the authentication process of Abacus ERP allows a remote attacker to bypass the second authenticati

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Abacus	Abacus Erp 2018	All	All	All	All
Application	Abacus	Abacus Erp 2019	All	All	All	All
Application	Abacus	Abacus Erp 2020	All	All	All	All
Application	Abacus	Abacus Erp 2021	All	All	All	All
Application	Abacus	Abacus Erp 2022	All	All	All	All

References

Reference	Source	Link	Tags
www.redguard.ch/advisories/abacus_mfa_bypass.txt	CONFIRM	www.redguard.ch	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Roman Gribi, Redguard AG

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](#)