



CVE-2022-0016

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

Summary

CVE	CVE-2022-0016
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-10 18:15:00 UTC
Updated	2022-02-17 13:54:00 UTC
Description	An improper handling of exceptional conditions vulnerability exists within the Connect Before Logon feature of the Palo Alto

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Paloaltonetworks	Globalprotect	All	All	All	All

References

Reference	Source	Link
CVE-2022-0016 GlobalProtect App: Privilege Escalation Vulnerability When Using Connect Before Logon	CONFIRM	security.paloaltonetv
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks Adam Crosser (Praetorian), Brian Sizemore (Praetorian) and N. Sao (Genetec) for independently discovering and reporting this issue.

Legacy QID Mappings

376413 Palo Alto Networks (GlobalProtect App) Privilege Escalation Vulnerability (GPC-14404, GPC-13685, GPC-14747)

© [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](#).

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