



CVE-2022-0018

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-0018
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 15:10:00 UTC
Description	An information exposure vulnerability exists in the Palo Alto Networks GlobalProtect app on Windows and MacOS where th

Risk And Classification

Problem Types: CWE-200

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

[CVE-2022-0018 GlobalProtect App: Information Exposure Vulnerability When Connecting to GlobalProtect Portal With Single Sign-On Enable](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks Irina Belyaeva of Jet Infosystems for discovering and reporting this issue.

Legacy QID Mappings

[376412](#) Palo Alto Networks (GlobalProtect App) Information Exposure Vulnerability (GPC-14203)

© [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](#)