



CVE-2020-2032

Published on: 06/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:07 PM UTC

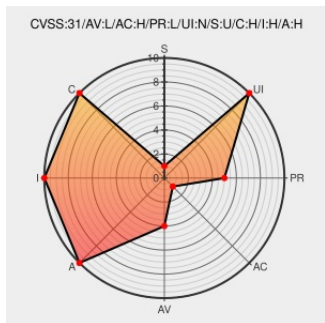
CVE-2020-2032

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Globalprotect](#) from [Paloaltonetworks](#) contain the following vulnerability:

A race condition vulnerability Palo Alto Networks GlobalProtect app on Windows allows a local limited Windows user to execute programs with SYSTEM privileges. This issue can be exploited only while performing a GlobalProtect app upgrade. This issue affects: GlobalProtect app 5.0 versions earlier than GlobalProtect app 5.0.10 on Windows; GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.4 on Windows.

CVE-2020-2032 has been assigned by [psirt@paloaltonetworks.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Palo Alto Networks](#) - **GlobalProtect App** version < 5.1.4

Affected Vendor/Software: [Palo Alto Networks](#) - **GlobalProtect App** version !>= 5.1.4

Affected Vendor/Software: [Palo Alto Networks](#) - **GlobalProtect App** version < 5.0.10

Affected Vendor/Software: [Palo Alto Networks](#) - **GlobalProtect App** version !>= 5.0.10

CVSS3 Score: **7 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

CVE-2020-2032 GlobalProtect App: File race condition vulnerability leads to local privilege escalation during upgrade

Vendor Advisory

[security.paloaltonetworks.com](https://security.paloaltonetworks.com/text/html)

text/html

 MISCsecurity.paloaltonetworks.com/CVE-2020-2032

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[375751](#) GlobalProtect App on Windows Privilege Escalation Vulnerability

[375826](#) Palo Alto GlobalProtect App Multiple Vulnerabilities

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Globalprotect	All	All	All	All
Application	Paloaltonetworks	Globalprotect	All	All	All	All
cpe:2.3:a:paloaltonetworks:globalprotect:*:*:*:*:windows:*:*:						
cpe:2.3:a:paloaltonetworks:globalprotect:*:*:*:*:windows:*:*:						

Discovery Credit

Palo Alto Networks thanks Rich Mirch of TeamARES from Critical Start Inc for discovering and reporting this issue.

[← Previous ID](#)[Next ID →](#)© CVE.report 2023   |

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](#)