



NATIONAL VULNERABILITY DATABASE



VULNERABILITIES

CVE-2024-3400 Detail

Description

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



Base Score: 10.0 CRITICAL

CNA: Palo Alto

Networks, Inc.

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites 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 web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://security.paloaltonetworks.com/CVE-2024-3400	Vendor Advisory
https://unit42.paloaltonetworks.com/cve-2024-3400/	Exploit Vendor Advisory
https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	Technical Description Vendor Advisory
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/	Exploit Third Party Advisory


This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference [CISA's BOD 22-01](#) and [Known Exploited Vulnerabilities Catalog](#) for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Palo Alto Networks PAN-OS Command Injection Vulnerability	04/12/2024	04/19/2024	Apply mitigations per vendor instructions as they become available. Otherwise, users with vulnerable versions of affected devices should

		enable Threat Prevention IDs available from the vendor. See the vendor bulletin for more details and a patch release schedule.
--	--	--




Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	 NIST Palo Alto Networks, Inc.
CWE-20	Improper Input Validation	Palo Alto Networks, Inc.

Known Affected Software Configurations [Switch to CPE](#)

2.2

Configuration 1 ([hide](#))

 cpe:2.3:o:paloaltonetworks:pan-os:10.2.0:-:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.0:h1:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.0:h2:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.0:h3:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.1:-:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.1:h1:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.1:h2:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.2:-:*:*:*:*:* Show Matching CPE(s) ▼
 cpe:2.3:o:paloaltonetworks:pan-os:10.2.2:h1:*:*:*:*:* Show Matching CPE(s) ▼

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.2:h2:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.2:h4:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.2:h5:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.3:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.3:h11:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.3:h12:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.3:h13:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.3:h2:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.3:h4:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.3:h9:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.4:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.4:h10:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.4:h16:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.4:h2:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.4:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.4:h4:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🚧 cpe:2.3:o:paloaltonetworks:pan-os:10.2.5:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.5:h1:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.5:h4:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.5:h6:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.6:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.6:h1:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.6:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.7:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.7:h1:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.7:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.7:h6:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.7:h8:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.8:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.8:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.9:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:10.2.9:h1:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.0:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.0:h1:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.0:h2:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.0:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.1:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.1:h2:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.1:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.1:h4:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.2:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.2:h1:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.2:h2:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.2:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.2:h4:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.3:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.3:h1:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.3:h10:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.3:h3:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)


🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.3:h5:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

🔌 cpe:2.3:o:paloaltonetworks:pan-os:11.0.4:-:*:*:*:*:*

[Show Matching CPE\(s\)▼](#)

 cpe:2.3:o:paloaltonetworks:pan-os:11.0.4:h1:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.0:-:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.0:h1:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.0:h2:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.0:h3:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.1:-:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.1:h1:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.2:-:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.2:h1:*:*:*:* Show Matching CPE(s)▼
 cpe:2.3:o:paloaltonetworks:pan-os:11.1.2:h3:*:*:*:* Show Matching CPE(s)▼

 Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

14 change records found [show changes](#)

QUICK INFO

CVE Dictionary Entry:

CVE-2024-3400

NVD Published Date:

04/12/2024

NVD Last Modified:

05/29/2024

Source:

Palo Alto Networks, Inc.



HEADQUARTERS

100 Bureau Drive
Gaithersburg, MD 20899
(301) 975-2000

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)

**Incident Response Assistance and Non-NVD
Related**

Technical Cyber Security Questions:

US-CERT Security Operations Center

Email: soc@us-cert.gov

Phone: 1-888-282-0870

[Site Privacy](#) | [Accessibility](#) | [Privacy Program](#) | [Copyrights](#) | [Vulnerability Disclosure](#) | [No Fear Act Policy](#) | [FOIA](#) | [Environmental Policy](#) |
[Scientific Integrity](#) | [Information Quality Standards](#) | [Commerce.gov](#) | [Science.gov](#) | [USA.gov](#)