NCSC
National Cyber Security Centre

2404120137-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical OS Command Injection Vulnerability in Palo Alto GlobalProtect Feature - CVE-2024-3400 (CVSS 10.0)

UPDATE

Wednesday 17th April, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Revision History

Revision	Date	Author(s)	Description
1.0	12th April 2024	CSIRT-IE	Initial advisory released
1.1	15th April 2024	CSIRT-IE	Details of Hot Fixes included
1.2	17th April 2024	CSIRT-IE	Update on previous mitigations and hotfix release dates

Description

Published: 12th April 2024
Vendor: Palo Alto Networks
Product: PAN-OS Cloud NGFW Prisma Access
CVSS 4.0 Score[1]**:** 10.0
EPSS[2]**:** 0.955770000 (For up to date EPSS score, click here: `https://api.first.org/data/v1/epss?cve=CVE-2024-3400`)
Summary: CVE-2024-3400 is a command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software. It may allow an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Palo Alto Networks is aware of a limited number of attacks that leverage the exploitation of this vulnerability.

Please note that the NCSC is aware of multiple cases of exploitation of this vulnerability meaning, those organisations who used the workaround instead of the patch, should now conduct an incident response process in all the cases.

Products Affected

The following products are affected:

- PAN-OS 11.1
- PAN-OS 11.0
- PAN-OS 10.2

Cloud NGFW, Panorama appliances, and Prisma Access **are not impacted** by this vulnerability.

Impact

A command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software and may allow an unauthenticated attacker to execute arbitrary code with root privileges on vulnerable firewalls.

Disabling device telemetry is **no longer** an effective mitigation. Device telemetry does not need to be enabled for PAN-OS firewalls to be exposed to attacks related to this vulnerability.The vulnerability is being actively exploited.

Recommendations

The NCSC strongly advises affected organisations to identify any affected products and upgrade to the latest fixes as soon as possible. More details are available in the Palo Alto Network Security Advisory which can be found here:

[1] https://www.first.org/cvss/v4.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins

- https://security.paloaltonetworks.com/CVE-2024-3400
- https://unit42.paloaltonetworks.com/cve-2024-3400/
- https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/
- https://attackerkb.com/topics/SSTk336Tmf/cve-2024-3400/rapid7-analysis

HotFixes for PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 are now released and are available to install. The NCSC-IE strongly recommends to install any hotfixes that apply to any of your deployments as soon as possible.

Details of further hotfix releases can be seen below:

PAN-OS 10.2:

- 10.2.9-h1 (Released 4/14/24)
- 10.2.8-h3 (ETA: 4/15/24)
- 10.2.7-h8 (ETA: 4/15/24)
- 10.2.6-h3 (ETA: 4/16/24)
- 10.2.5-h6 (ETA: 4/16/24)
- 10.2.3-h13 (ETA: 4/17/24)
- 10.2.1-h2 (ETA: 4/17/24)
- 10.2.2-h5 (ETA: 4/18/24)
- 10.2.0-h3 (ETA: 4/18/24)
- 10.2.4-h16 (ETA: 4/19/24)

PAN-OS 11.0:

- 11.0.4-h1 (Released 4/14/24)
- 11.0.3-h10 (ETA: 4/16/24)
- 11.0.2-h4 (ETA: 4/16/24)
- 11.0.1-h4 (ETA: 4/17/24)
- 11.0.0-h3 (ETA: 4/18/24)

PAN-OS 11.1::

- 11.1.2-h3 (Released 4/14/24)
- 11.1.1-h1 (ETA: 4/16/24)
- 11.1.0-h3 (ETA: 4/16/24)

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie