CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect

Severity 10 · CRITICAL

Urgency **HIGHEST**	Response Effort **MODERATE**	Recovery **USER**	Value Density **CONCENTRATED**
Attack Vector **NETWORK**	Attack Complexity **LOW**	Attack Requirements **NONE**	Automatable **YES**
User Interaction **NONE**	Product Confidentiality **HIGH**	Product Integrity **HIGH**	Product Availability **HIGH**
Privileges Required **NONE**	Subsequent Confidentiality **HIGH**	Subsequent Integrity **HIGH**	Subsequent Availability **HIGH**

NVD JSON

Published **2024-04-12**

Updated **2024-05-03**

Reference **PAN-252214**

Discovered **in production use**

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.

Customers should continue to monitor this security advisory for the latest updates and product guidance.

Product Status

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.1	< 11.1.0-h3, < 11.1.1-h1, < 11.1.2-h3	>= 11.1.0-h3, >= 11.1.1-h1, >= 11.1.2-h3
PAN-OS 11.0	< 11.0.0-h3, < 11.0.1-h4, < 11.0.2-h4, < 11.0.3-h10, < 11.0.4-h1	>= 11.0.0-h3, >= 11.0.1-h4, >= 11.0.2-h4, >= 11.0.3-h10, >= 11.0.4-h1

PAN-OS 10.2	< 10.2.0-h3, < 10.2.1-h2, < 10.2.2-h5, < 10.2.3-h13, < 10.2.4-h16, < 10.2.5-h6, < 10.2.6-h3, < 10.2.7-h8, < 10.2.8-h3, < 10.2.9-h1	>= 10.2.0-h3, >= 10.2.1-h2, >= 10.2.2-h5, >= 10.2.3-h13, >= 10.2.4-h16, >= 10.2.5-h6, >= 10.2.6-h3, >= 10.2.7-h8, >= 10.2.8-h3, >= 10.2.9-h1
PAN-OS 10.1	None	All
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
PAN-OS 9.0	None	All
Prisma Access	None	All

Required Configuration for Exposure

This issue is applicable only to PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls configured with GlobalProtect gateway or GlobalProtect portal (or both). Device telemetry does not need to be enabled for PAN-OS firewalls to be exposed to attacks related to this vulnerability.

You can verify whether you have a GlobalProtect gateway or GlobalProtect portal configured by checking for entries in your firewall web interface (Network > GlobalProtect > Gateways or Network > GlobalProtect > Portals).

Severity: CRITICAL

CVSSv4.0 Base Score: 10 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/AU:Y/R:U/V:C/RE:M/U:Red)

Exploitation Status

Palo Alto Networks is aware of an increasing number of attacks that leverage the exploitation of this vulnerability. Proof of concepts for this vulnerability have been publicly disclosed by third parties.

We are also aware of proof-of-concept by third parties of post-exploit persistence techniques that survive resets and upgrades. We are not aware at this time of any malicious attempts to use these persistence techniques in active exploitation of the vulnerability. These fixes listed below and Threat Prevention signatures completely prevent the initial remote command execution, stopping subsequent post-exploitation or persistence.

More information about the vulnerability's exploitation in the wild can be found in the Unit 42 threat brief (https://unit42.paloaltonetworks.com/cve-2024-3400/) and the Palo Alto Networks PSIRT blog post (https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/).

Weakness Type

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

CWE-20 Improper Input Validation

Solution

We strongly advise customers to immediately upgrade to a fixed version of PAN-OS to protect their devices even when workarounds and mitigations have been applied.

This issue is fixed in PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, PAN-OS 11.1.2-h3, and in all later PAN-OS versions. These fixes and those listed below completely prevent the initial remote command execution, stopping subsequent post-exploitation or persistence.

In addition, to provide the most seamless upgrade path for customers, additional hotfixes have been made available as a courtesy for other commonly deployed maintenance releases.

```
PAN-OS 10.2:
- 10.2.9-h1 (Released 4/14/24)
- 10.2.8-h3 (Released 4/15/24)
- 10.2.7-h8 (Released 4/15/24)
- 10.2.6-h3 (Released 4/16/24)
- 10.2.5-h6 (Released 4/16/24)
- 10.2.4-h16 (Released 4/18/24)
- 10.2.3-h13 (Released 4/18/24)
- 10.2.2-h5 (Released 4/18/24)
- 10.2.1-h2 (Released 4/18/24)
- 10.2.0-h3 (Released 4/18/24)

PAN-OS 11.0:
- 11.0.4-h1 (Released 4/14/24)
- 11.0.4-h2 (Released 4/17/24)
- 11.0.3-h10 (Released 4/16/24)
- 11.0.2-h4 (Released 4/16/24)
- 11.0.1-h4 (Released 4/18/24)
- 11.0.0-h3 (Released 4/18/24)

PAN-OS 11.1:
- 11.1.2-h3 (Released 4/14/24)
- 11.1.1-h1 (Released 4/16/24)
- 11.1.0-h3 (Released 4/16/24)
```

Note: Due to naming convention limitations, “-h” hotfix versions on Azure marketplace are instead named via addition of an extra “0”. Ex: 11.1.2-h3 is published on Azure as 11.1.203.

If any exploitation was observed on a device, please take the remediation steps suggested here: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CrO6CAK

An enhanced factory reset (EFR) procedure that does not rely on the integrity of a potentially compromised device can be scheduled by opening a case through Customer Support (TAC). This is recommended for:

1. Customers who have not applied the PAN-OS fixes or Threat Prevention signatures with vulnerability protection applied to the GlobalProtect interface (regardless of level of compromise) on or before April 25, 2024; or

2. Customers who are concerned about a persistent risk.

Workarounds and Mitigations

Recommended Mitigation: Customers with a Threat Prevention subscription can block attacks for this vulnerability using Threat IDs 95187, 95189, and 95191 (available in Applications and Threats content version 8836-8695 and later). Please monitor this advisory and new Threat Prevention content updates for additional Threat Prevention IDs around CVE-2024-3400.

To apply the Threat IDs, customers must ensure that vulnerability protection has been applied to their GlobalProtect interface to prevent exploitation of this issue on their device. Please see https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184 for more information.

In earlier versions of this advisory, disabling device telemetry was listed as a secondary mitigation action. 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.

Acknowledgments

Palo Alto Networks thanks Volexity for detecting and identifying this issue, Capability Development Group at Bishop Fox for helping us improve threat prevention signatures, Nick Wilson, and Louis Lingg for sharing their research into post-exploitation persistence techniques.

Frequently Asked Questions

Q.Has this issue been exploited in the wild?

Palo Alto Networks is aware of an increasing number of attacks that leverage the exploitation of this vulnerability. Proof of concepts for this vulnerability have been publicly disclosed by third parties.

We are also aware of proof of concepts by third parties of post-exploit persistence techniques that survive resets and upgrades. These techniques work on a device that is already compromised with interactive root level command execution.

Q.Are there any checks I can run on my device to look for evidence of attempted exploit activity?

The following command can be used from the PAN-OS CLI to help identify if there was an attempted exploit activity on the device:

```
grep pattern "failed to unmarshal session(.\+.\/" mp-log gpsvc.log*
```

If the value between "session(" and ")" does not look like a GUID, but instead contains a file system path or embedded shell commands, this could be related to an attempted exploitation of CVE-2024-3400, which will warrant further investigation to correlate with other indicators of compromise.

Grep output indicating an attempted exploit may look like the following entry:

```
failed to unmarshal session(../../some/path)
```

Grep output indicating normal behavior will typically appear like the following entry:

```
failed to unmarshal session(01234567-89ab-cdef-1234-567890abcdef)
```

Q.When should I collect a Tech Support File (TSF) and forensic evidence during the upgrade process?

You should obtain a TSF for forensic analysis before rebooting into a fixed version of PAN-OS. If you have already upgraded the firewall, but did not collect a TSF, some logs from the prior system installation will become inaccessible on the device. Please reach out to support if you need help investigating a prior PAN-OS installation.

Q.Has my device been compromised by this vulnerability?

Customers are able to open a case in the Customer Support Portal (CSP) and upload a technical support file (TSF) to determine if their device logs match known attempted exploits for this vulnerability.

Q.How do I verify I applied the Threat Prevention signatures correctly?

Run the following command against the GlobalProtect enabled PAN-OS 10.2+ firewall:

```
curl -v -k -H "Cookie: SESSID=/../TESTVULN" https://<target-host>/global-protect/login.esp
```

If the firewall is protected by the necessary Threat Prevention signatures, no response will be returned. A TCP reset will occur. A successful response indicates that Threat Prevention signatures are not correctly applied. Please follow the steps in https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184

Q.Where can I find additional indicators of compromise for this issue?

Please refer to the Unit42 Threat Brief (https://unit42.paloaltonetworks.com/cve-2024-3400/) and the Volexity blog post (https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/) for the latest information.

Q.Are VMs deployed and managed by customers in the cloud impacted?

While the Cloud NGFW managed services on AWS and Azure are not impacted, VM-Series managed by customers and with specific PAN-OS versions and Global Protect configurations are impacted.

Timeline

2024-05-03 Enhanced Factory Reset (EFR) Procedure is Available Against any Potential Post-Exploit Persistence Techniques.

2024-05-01 Answered a FAQ about how to verify the fix or threat prevention signature was applied correctly

2024-04-29 Updated exploitation status about proof-of-concept by third parties of post-exploit persistence techniques

2024-04-25 Added link to KB article for remediating a device

2024-04-20 Answered a FAQ about Tech Support File collection and forensic evidence

2024-04-19 Added reference to PSIRT blog post about CVE-2024-3400

2024-04-19 Clarified vulnerability title and description

2024-04-17 Clarified FAQ regarding evidence of attempted exploit activity

2024-04-17 Added new Threat Prevention Threat ID to Workarounds and Mitigations

2024-04-17 Added a CLI command to search for possible attempts of exploit activity

2024-04-16 Updated product and mitigation guidance, exploit status, and PAN-OS fix availability

2024-04-15 All necessary PAN-OS fixes are now available, clarified Workarounds and Mitigations when using Panorama templates

2024-04-14 Clarified impact on GlobalProtect portal configurations

2024-04-13 Added link to Unit42 threat brief and clarified impact to customer-managed VMs in the cloud

2024-04-12 Initial publication