CVE-2024-9474

Description

A privilege escalation vulnerability identified in Palo Alto Networks PAN-OS software, enabling a PAN-OS administrator with management web interface access to execute actions on the firewall with root-level privileges via a Command Injection.

Metrics

Authority	CVSS Version	CVSS B	Vector
CNA: Palo Alto Networks, Inc.	4.0	6.9 (Medium)	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/ UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/ AU:N/R:U/V:C/RE:H/U:Red
NIST: NVD	3.x	7.2 (High)	CVSS:3.1/AV:N/AC:L/PR:H/ UI:N/S:U/C:H/I:H/A:H

Potential Impact

Exploiting this vulnerability can lead to full system compromise, allowing the attacker to alter firewall configurations, access sensitive data, and disrupt network operations, impacting system integrity and security.

Software versions affected

Software versions impacted by the vulnerability are listed below:

- PAN-OS 11.2: versions < 11.2.4-h1.
- PAN-OS 11.1: versions < 11.1.5-h1.
- PAN-OS 11.0: versions < 11.0.6-h1.
- PAN-OS 10.2: versions < 10.2.12-h2.
- PAN-OS 10.1: versions < 10.1.14-h6.

It impacts the software on PA-Series, VM-Series, CN-Series firewalls, and on Panorama (virtual and M-Series) and WildFire appliances. It does not affect Palo Alto's Prisma Access and Cloud NGFW solutions.

Remediation measures

According to vendor this vulnerability is fixed in PAN-OS versions 10.1.14-h6, 10.2.12-h2, 11.0.6-h1, 11.1.5-h1, 11.2.4-h1, and later. Users are urged to update to a patched version. Also, restricting management interface access to trusted internal IPs is recommended in order to reduce the potential attack surface.

Potential Exploitation

The vulnerability can be exploited by manipulating the `user` parameter in POST request sent to a specific endpoint on a management web interface. An example exploitation chain would be as follows:

1. Send a POST request to `/php/utils/createRemoteAppwebSession.php/X.js.map` with `user` parameter set to the desired command e.g., `echo $(uname -a) > /var/appweb/htdocs/unauth/X.php`, as an authenticated user.
2. Send a GET request to `/index.php/.js.map` as an authenticated user in order to execute the injected command.
3. Send a GET request to `/unauth/X.php` as an authenticated user to collect command's output.

One can also exploit CVE-2024-0012 vulnerability to bypass the authentication.

References

- `https://security.paloaltonetworks.com/CVE-2024-9474`
- `https://nvd.nist.gov/vuln/detail/CVE-2024-9474`
- `https://github.com/k4nfr3/CVE-2024-9474`
- `https://labs.watchtowr.com/pots-and-pans-aka-an-sslvpn-palo-alto-pan-os-cve-2024-0012-and-cve-2024-9474/`

CVE-2024-0012

Description

An authentication bypass vulnerability identified in Palo Alto Networks PAN-OS software, enabling an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges and perform administrative actions.

Metrics

Authority	CVSS Version	CVSS B	Vector
CNA: Palo Alto Networks, Inc.	4.0	9.3 (Critical)	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/ UI:N/VC:H/VI:H/VA:H/SC:L/SI:N/SA:N/ AU:N/R:U/V:C/RE:H/U:Red
NIST: NVD	3.x	9.8 (Critical)	CVSS:3.1/AV:N/AC:L/PR:N/ UI:N/S:U/C:H/I:H/A:H

Potential Impact

Exploiting this vulnerability allows an unauthenticated attacker to gain PAN-OS administrator privileges, allowing them to perform administrative actions, alter critical configurations, and potentially exploit other authenticated privilege escalation vulnerabilities, such as CVE-2024-9474.

Software versions affected

Software versions impacted by the vulnerability are listed below:

- PAN-OS 11.2: versions < 11.2.4-h1.
- PAN-OS 11.1: versions < 11.1.5-h1.
- PAN-OS 11.0: versions < 11.0.6-h1.
- PAN-OS 10.2: versions < 10.2.12-h2.

It impacts the software on PA-Series, VM-Series, CN-Series firewalls, and on Panorama (virtual and M-Series). It does not affect Palo Alto's PAN-OS version 10.1, Prisma Access and Cloud NGFW solutions.

Remediation measures

According to vendor this vulnerability is fixed in PAN-OS versions 10.2.12-h2, 11.0.6-h1, 11.1.5-h1, 11.2.4-h1, and later. Users are urged to update to a patched version. Also, restricting management interface access to trusted internal IPs is recommended in order to reduce the potential attack surface. Vulnerability exploitation can be mitigated by using Threat IDs 95746, 95747, 95752, 95753, 95759, and 95763, provided the user has a Threat Prevention subscription, by ensuring the following:

- All listed Threat IDs are set to block mode.
- MGT port traffic is routed through a DP port by enabling a management profile on a DP interface.
- Inbound traffic management certificate is replaced.
- Inbound traffic to the management interface is decrypted for inspection.
- Threat prevention on inbound traffic to management services is enabled.

Potential Exploitation

The vulnerability can be exploited by setting the `X-PAN-AUTHCHECK` parameter to `off` in a HTTP request.

References

- `https://security.paloaltonetworks.com/CVE-2024-0012`
- `https://nvd.nist.gov/vuln/detail/CVE-2024-0012`
- `https://labs.watchtowr.com/pots-and-pans-aka-an-sslvpn-palo-alto-pan-os-cve-2024-0012-and-cve-2024-9474/`