AL2024_39 Over 2,000 Palo Alto Firewalls Compromised Using Recently Patched Zero-Day Vulnerabilities (29th November 2024)

Description

Hackers have exploited two recently patched zero-day vulnerabilities in Palo Alto Networks PAN-OS software, compromising over 2,000 firewalls worldwide. The vulnerabilities CVE-2024-0012 (authentication bypass) and CVE-2024-9474 (privilege escalation) enable attackers to gain administrator privileges and execute commands with root access. While Palo Alto Networks initially flagged these issues earlier in November, ongoing attacks have intensified, highlighting the urgency for organizations to secure their devices.

Attack Details

A recently disclosed series of vulnerabilities in Palo Alto Networks' PAN-OS has enabled attackers to exploit critical flaws in the management web interface, resulting in significant security incidents. Two key vulnerabilities, CVE-2024-0012 (an authentication bypass) and CVE-2024-9474 (a privilege escalation flaw), are being chained together to allow attackers to gain unauthorized administrator access and execute commands with root privileges on compromised firewalls. These vulnerabilities have facilitated the complete takeover of targeted devices.

The issue gained attention on November 8, 2024, when Palo Alto Networks issued an advisory warning customers to restrict management web interface access due to a potential remote code execution (RCE) risk. By November 18, exploitation activities were detected, and by November 21, Shadowserver reported over 2,000 compromised devices. The attack primarily targets devices with exposed management interfaces, leveraging anonymous VPN services to conceal attackers' origins. Shadowserver has identified a total of 2,700 vulnerable devices, underscoring the widespread impact despite Palo Alto Networks downplaying the scale of the incident.

Organizations using affected devices are urged to act swiftly to mitigate these vulnerabilities by securing web interfaces, applying patches, and implementing strict access controls to prevent further exploitation.

Remediation

To mitigate the risks and secure devices, organizations should take the following actions:

- Patch Systems: Immediately apply updates for CVE-2024-0012 and CVE-2024-9474.
- Restrict Access: Limit management web interface access to trusted internal IPs and follow best practice deployment guidelines.

- Secure Configurations: Ensure management interfaces are not internet-facing, audit access permissions, and minimize privileges.
- Monitor for Threats: Use tools like Shadowserver to detect vulnerabilities or compromises.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2024, November 21). Over 2,000 Palo Alto firewalls were hacked using recently patched bugs. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/over-2-000-palo-alto-firewalls-hacked-using-recently-patched-bugs/
- Page, C. (2024, November 21). Palo Alto Networks warns hackers are breaking into its customers' firewalls — again. Retrieved from TechCrunch. https://techcrunch.com/2024/11/21/palo-alto-networks-warns-hackers-are-breaking-into-its-customers-firewalls-again/