September 14, 2023

Overall rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Palo Alto Networks vulnerability. Included were updates for the following:

- PAN-OS 0 – versions prior to 11.0.3
- PAN-OS 10.2 – versions prior to 10.2.6
- PAN-OS 10.1 – versions prior to 10.1.11
- PAN-OS 9.1 – version 9.1.16 and prior

Technical Details

BGP software such as FRRouting FRR included as part of the PAN-OS virtual routing feature enables a remote attacker to incorrectly reset network sessions though an invalid BGP update. This issue is applicable only to firewalls configured with virtual routers that have BGP enabled.

This issue requires the remote attacker to control at least one established BGP session that is propagated to the PAN-OS virtual router to exploit it. The denial-of-service (DoS) impact on the network is dependent on the network's architecture and fault tolerant design.

Further details about this issue can be found at: https://blog.benjojo.co.uk/post/bgp-path-attributes-grave-error-handling

Exploitability Metrics

Attack Vector: Local

Attack Complexity: High

Privileges Required: High

User Interaction: None

This vulnerability is rated as a **high** risk. A software update exists to address this risk.

Action Required

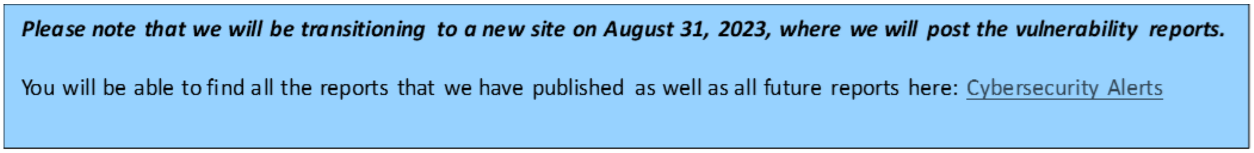
- Locate the device or application and investigate.

- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- **CVE-2023-38802**
- Palo Alto Networks Security Advisory - CVE-2023-38802



Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts