Security Advisory 2021-048

Vulnerabilities in PaloAlto Software

September 10, 2021 — v1.0

TLP:WHITE

Summary

On September 8, Palo Alto published security advisories about three vulnerabilities rated as *high* [1], CVE-2020-10188 [2], CVE-2021-3051 [3] and CVE-2021-3052 [4] affecting respectively PanOS telnet-based administrative management service, Cortex XSOAR and PAN-OS web interface.

Technical Details

CVE-2020-10188 - CVSSv3.1 Score: 8.1

The vulnerability identified as CVE-2020-10188 allows remote attackers to execute arbitrary code due to a buffer overflow vulnerability in the telnet-based administrative management service included with PAN-OS software. This issue is exploitable only if the telnet service is enabled and is accessible to attackers [2].

CVE-2021-3051 - CVSSv3.1 Score: 8.1

The vulnerability identified as CVE-2021-3051 allows an unauthenticated network-based attacker with specific knowledge of the Cortex XSOAR instance to access protected resources and perform unauthorised actions on the Cortex XSOAR server due to an improper verification of cryptographic signature vulnerability exists in Cortex XSOAR SAML authentication [3].

CVE-2021-3052 - CVSSv3.1 Score: 8

The vulnerability identified as CVE-2021-3052 allows an authenticated network-based attacker to mislead another authenticated PAN-OS administrator to click on a specially crafted link that performs arbitrary actions in the PAN-OS web interface as the targeted authenticated administrator due to a reflected cross-site scripting (XSS) vulnerability in the Palo Alto Network PAN-OS web interface [4].

Palo Alto Networks is not aware of any malicious attempts to exploit these vulnerabilities.

Products Affected

The following product versions are affected:

CVE-2020-10188

Versions	Affected	Unaffected
PAN-OS 10.1	None	10.1.*
PAN-OS 10.0	< 10.0.6	>= 10.0.6
PAN-OS 9.1	< 9.1.9	>= 9.1.9
PAN-OS 9.0	< 9.0.14	>= 9.0.14
PAN-OS 8.1	< 8.1.20	>= 8.1.20

CVE-2021-3051

Versions	Affected	Unaffected
Cortex XSOAR 6.2.0	< 1578666	>=1578666
Cortex XSOAR 6.1.0	< 1578663	>= 1578663
Cortex XSOAR 6.0.2	< 1576452	>= 1576452
Cortex XSOAR 5.5.0	< 1578677	>= 1578677

CVE-2021-3052

Versions	Affected	Unaffected
PAN-OS 10.1	None	10.1.*
PAN-OS 10.0	< 10.0.2	>= 10.0.2
PAN-OS 9.1	< 9.1.10	>= 9.1.10
PAN-OS 9.0	< 9.0.14	>= 9.0.14
PAN-OS 8.1	< 8.1.20	>= 8.1.20

Recommendations

For CVE-2020-10188, Palo Alto recommends updating to PAN-OS 8.1.20, PAN-OS 9.0.14, PAN-OS 9.1.9, PAN-OS 10.0.6, and all later PAN-OS versions.

For CVE-2021-3051, Palo Alto recommends updating to Cortex XSOAR 5.5.0 build 1578677, Cortex XSOAR 6.0.2 build 1576452, Cortex XSOAR 6.1.0 build 1578663, Cortex XSOAR 6.2.0 build 1578666, and all later Cortex XSOAR versions.

For CVE-2021-3052, Palo Alto recommends updating to PAN-OS 9.0.14, PAN-OS 8.1.20, PAN-OS 9.1.10, PAN-OS 10.0.2, PAN-OS 10.1.0, and all later PAN-OS versions.

Mitigations

CVE-2020-10188 is mitigated by disabling the telnet-based administrative management service. This completely eliminates risks of exploitation of this issue. If the telnet-based administrative management service is required and you cannot immediately upgrade your PAN-OS software, enable signatures for Unique Threat ID 59125 on traffic destined for the telnet interface to block attacks using this vulnerability.

CVE-2021-3051 is completely prevented by disabling SAML authentication integration. The

network access to Cortex XSOAR server can be restricted to allow only trusted users to further reduce the impact of this issue.

CVE-2021-3052 vulnerability requires the attacker to have authenticated access to the PAN-OS web interface. To mitigate the impact of this issue, best practices should be followed for securing the PAN-OS web interface [5].

References

[1] https://security.paloaltonetworks.com/

[2] https://security.paloaltonetworks.com/CVE-2020-10188

[3] https://security.paloaltonetworks.com/CVE-2021-3051

[4] https://security.paloaltonetworks.com/CVE-2021-3052

[5] https://docs.paloaltonetworks.com/best-practices