Security Advisory 2021-035

Multiple Palo Alto Vulnerabilities

July 15, 2021 — v1.0

TLP:WHITE

History:

- *15/07/2021 — v1.0 – Initial publication*

Summary

On July 14, Palo Alto published security advisories about two vulnerabilities rated as *high* [1], CVE-2021-3042 [2] and CVE-2021-3044 [4], affecting respectively Cortex XDR Agent and Prisma Cloud.

Technical details

CVE-2021-3042

The vulnerability identified as CVE-2021-3042 [2] allows authenticated local Windows users to run programs with SYSTEM privilege due to improper control of user-controlled file [3]. To exploit this vulnerability, the local user needs to have file creation privilege in the Windows Root Directory [2].

CVE-2021-3043

The vulnerability identified as CVE-2021-3043 [4] allows an attacker to exploit a reflected cross-site scripting (XSS) vulnerability [5] in the Prisma Cloud compute web console, enabling the attacker to execute arbitrary JavaScript code in the browser-based web console while an authenticated administrator is using that web interface.

Products affected

CVE-2021-3042

The following product versions are affected if they do not have content update 181 or later:

- Cortex XDR Agent 7.3
- Cortex XDR Agent 7.2
- Cortex XDR Agent 6.1

Cortex XDR Agent 5 is not affected at all.

CVE-2021-3043

Versions	Affected	Unaffected
Prisma Cloud Compute 21.04	Earlier version than 21.04.439	21.04.439 and later version
Prisma Cloud Compute 20.12	Earlier version than 20.12.552	20.12.552 and later version

Recommendations

Palo Alto recommends updating Cortex XDR agent 6.1, 7.2, 7.3, and all later Cortex XDR agent versions with content update 181 or later content updates.

Palo Alto recommends updating Prisma Cloud Compute to 20.12.552, 21.04.439, and all later Prisma Cloud Compute versions. Palo Alto also informed that Prisma Cloud Compute SaaS versions were automatically upgraded to the fixed release and so, no additional action is required for these instances.

Mitigations

CVE-2021-3042 is mitigated by preventing local authenticated Windows users from creating files in the Windows root directory.

References

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

[2] https://security.paloaltonetworks.com/CVE-2021-3042

[3] https://cwe.mitre.org/data/definitions/427

[4] https://security.paloaltonetworks.com/CVE-2021-3043

[5] https://cwe.mitre.org/data/definitions/79