CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-029

Critical Vulnerability in PaloAlto Cortex

June 24, 2021 — v1.0

TLP:WHITE

History:

- *24/06/2021 — v1.0 – Initial publication*

Summary

On the 22nd of June 2021, PaloAlto released Security Advisory to address a vulnerability in Palo Alto Networks Cortex XSOAR. Severity is **critical** with a CVSSv3.1 Base Score: 9.8 [1].

Technical Details

An improper authorisation vulnerability in some versions of Palo Alto Networks Cortex XSOAR enables a remote unauthenticated attacker with network access to the Cortex XSOAR server to perform unauthorised actions through the REST API [1].

The vulnerability received CVE-2021-3044 [2]

Products Affected

- Cortex XSOAR 6.1.0 builds later than 1016923 and earlier than 1271064;
- Cortex XSOAR 6.2.0 builds earlier than 1271065.

Recommendations

This issue is fixed in Cortex XSOAR 6.1.0 build 1271064, Cortex XSOAR 6.2.0 build 1271065, and all later Cortex XSOAR versions.

CERT-EU recommends updating the vulnerable application as soon as possible.

Workarounds and Mitigations

To fully mitigate the impact of this issue, all active integration API keys must be revoked.

To revoke integration API keys from the Cortex XSOAR web client go to *Settings* > *Integration* > *API Keys* and then *Revoke* each API key.

You can create new API keys after you upgrade Cortex XSOAR to a fixed version.

Restricting network access to the Cortex XSOAR server to allow only trusted users also reduces the impact of this issue. Please refer to [1] for more details.

References

[1] https://security.paloaltonetworks.com/CVE-2021-3044

[2] https://nvd.nist.gov/vuln/detail/CVE-2021-3044