CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-071

Palo Alto Critical Vulnerability

December 21, 2021 — v1.1

TLP:WHITE

History:

- *16/12/2021 — v1.0 – Initial publication*
- *21/12/2021 — v1.1 – Update PaloAlto affected products and recommendations*

Summary

On December 16th, Palo Alto updated its advisory related to CVE-2021-44228 affecting PAN-OS for Panorama [1]. While this CVE affects the Java logging library `log4j` [1], all products using this library are vulnerable *at least* to Unauthenticated Remote Code Execution [2].

On December 17th, Palo Alto included in its advisory the Exact Data Matching CLI to the list of the affected products.

On December 21st, Palo Alto released fixes for various versions of its products.

Technical Details

The vulnerability exists in the Java logging library log4j. An unauthenticated remote attacker might exploit this vulnerability by sending specially crafted content to the application to execute malicious code on the server [2]. This issue is due to ElasticSearch included in vulnerable version of PAN-OS, which uses log4j library.

Panorama hardwares and virtual appliances are vulnerable only if running in *Panorama mode* or *Log Collector mode* as part of a Collector group. To determine if the Panorama appliance is part of a Collector group, from the web interface, go to *Panorama -> Manage Collectors*.

Affected products

- PAN-OS for Panorama versions `<9.0.15`, `<10.0.8-h8`, and `<9.1.12-h3`
- Exact Data Matching CLI versions `<1.2`

Recommendations

Palo Alto recommends upgrading the Panorama appliance to the latest fixed release (versions `>=9.0.15`, `>=10.0.8-h8`, or `>=9.1.12-h3`). Palo Alto also recommends upgrading Exact Data Matching CLI to the version 1.2 or higher.

Notes:

- PAN-OS `8.1.*` for Panorama is not vulnerable
- PAN-OS `10.1.*` for Panorama is not vulnerable

Workarounds and Mitigations

As a workaround, Palo Alto recommends to remove the Panorama appliance from any Collector groups, from the web interface *Panorama* -> *Manage Collectors*. Once restarted, it stops using ElasticSearch which eliminates the exposure to CVE-2021-44228.

As mitigation, Palo Alto also recommends to use ACLs to limit the network access to Panorama to only trusted users, networks and IP addresses. To do so, use App-ID for `ldap` and `rmi-iiop` to block all LDAP and RMI from untrusted networks or unexpected sources.

References

[1] https://security.paloaltonetworks.com/CVE-2021-44228

[2] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf