CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-076

Fortinet Critical Vulnerability

December 18, 2021 — v1.0

TLP:WHITE

History:

- *18/12/2021 — v1.0 – Initial publication*

Summary

On December 15th, Fortinet PSIRT updated its advisory related to CVE-2021-44228 and CVE-2021-45046 affecting Fortinet products [1]. While these CVE affect the Java logging library `log4j`, all products using this library are vulnerable to Unauthenticated Remote Code Execution [2].

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].

Affected products and fixed versions

Affected product	Fixed version
FortiAIOps	1.0.2
FortiCASB	Fixed on 2021-12-10
FortiConverter Portal	Fixed on 2021-12-10
FortiCWP	Fixed on 2021-12-10
FortiEDR Cloud	Not exploitable. Additional precautionary mitigations put in place on 2021-12-10
FortiInsight	Not exploitable. Additional precautionary mitigations being investigated.
FortiIsolator	Fix scheduled for version 2.3.4
FortiMonitor	Mitigations for NCM [3] & Elastiflow [4] available
FortiPortal	Fixed in 6.0.8 and 5.3.8
FortiSIEM	Mitigation available [5]
ShieldX	Fix scheduled for versions 2.1 and 3.0 - ETA 2021/12/17

Recommendations

CERT-EU recommends applying the fixes or the mitigation provided by Fortinet PSIRT as soon as possible. Additionally, the Fortinet PSIRT provide:

- IPS Signature protection (FortiOS): VID 51006
- IPS Signature protection (FortiADC & FortiProxy): version 19.215
- Web Application Firewall Signature (FortiWeb & FortiWeb Cloud): database > 0.00305

Please note that IPS and WAF signatures are not sufficient to fully mitigate the vulnerabilities.

References

[1] https://www.fortiguard.com/psirt/FG-IR-21-245

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

[3] https://docs.fortinet.com/document/fortimonitor/21.4.0/user-guide/733336/technical-tip-mitigating-log4j-vulnerability-impact-on-ncm

[4] https://docs.fortinet.com/document/fortimonitor/21.4.0/user-guide/411268/technical-tip-mitigating-log4j-vulnerability-impact-on-elastiflow-4-and-5