CERT-EU Security Advisory 2018-018

WebLogic Vulnerability Exploited In The Wild

July 26, 2018 — v1.0

History:

- *26/07/2018 — v1.0: Initial publication*

Summary

Recently Oracle released patches for vulnerability CVE-2018-2893. This vulnerability allows an unauthenticated attacker to compromise Oracle WebLogic Server. Exploits were published on GitHub and on other websites after the announcement of the security updates. There were reported attacks against vulnerable instances.

Technical Details

On the 18th of July 2018, Oracle released patches for vulnerability CVE-2018-2893 with an assigned CVSS score of 9.8. [1]

The vulnerability allows an unauthenticated attacker to remotely take control of a WebLogic Server. [1]

Details about this vulnerability were never made public by Oracle but only the patches. Exploits were published on GitHub and on other websites after the announced of the security updates. [2],[3],[4],[5]

There were reported attacks against vulnerable instances. [6],[7]

Products Affected

Oracle WebLogic servers running versions 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3 are known to be vulnerable.

Recommendations

- Apply the Oracle July 2018 updates as soon as possible, and especially the patches for CVE-2018-2893.
- Block external access to port 7001 as the flaw is exploited via this port.
- Use detection rules in monitoring devices as fore example sigma rule in [8].

References

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2893

[2] https://www.bleepingcomputer.com/news/security/attacks-on-oracle-weblogic-servers-detected-after-publication-of-poc-code/

[3] https://github.com/shengqi158/CVE-2018-2628

[4] https://github.com/anbai-inc/CVE-2018-2893/

[5] https://www.securityweek.com/recently-patched-oracle-weblogic-flaw-exploited-wild

[6] https://isc.sans.edu/forums/diary/Weblogic+Exploit+Code+Made+Public+CVE20182893/23896/

[7] http://blog.netlab.360.com/malicious-campaign-luoxk-is-actively-exploiting-cve-2018-2893/

[8] https://github.com/Neo23x0/sigma/blob/master/rules/web/web_cve_2018_2894_weblogic_exploit.yml