Security Advisory 2022-082

Multiple Vulnerabilities in SolarWinds Platform

December 1, 2022 — v1.0

TLP:CLEAR

History:

- *01/12/2022 — v1.0 – Initial publication*

Summary

On November 22, SolwarWinds released a patch note for SolarWinds Platform 2022.4 fixing 7 vulnerabilities including 4 high rated vulnerabilities that could lead to arbitrary commands executed [1].

Technical Details

There are 7 vulnerabilities fixed in SolarWinds Platform 2022.4 [1]:

- **CVE-2022-36957** - (CVSS 7.2 High) - This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands on the Main Poller of affected versions of the SolarWinds Platform;
- **CVE-2022-36958** - (CVSS 8.8 High) - Deserialization of Untrusted Data This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands on the Main Poller of affected versions of the SolarWinds Platform;
- **CVE-2022-36960** - (CVSS 8.8 High) - This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to escalate user privileges on affected versions of the SolarWinds Platform;
- **CVE-2022-36962** - (CVSS 7.2 High) - This vulnerability allows a remote adversary with complete control over the SolarWinds database to execute arbitrary commands on the Main Poller of affected versions of the SolarWinds Platform;
- **CVE-2022-36964** - (CVSS 8.8 High) - This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands on the Main Poller of affected versions of the SolarWinds Platform;
- **CVE-2022-36966** - (CVSS 5.9 Medium) - Users with Node Management rights were able to view and edit all nodes due to Insufficient control on URL parameter causing insecure direct object reference (IDOR) vulnerability in SolarWinds Platform 2022.3;
- **CVE-2022-38108** - (CVSS 7.2 High) - This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands on the Main Poller of affected versions of the SolarWinds Platform.

Affected Products

The following products are affected [1]:

- SolarWinds Platform 2022.3 and earlier;
- Orion Platform 2020.2.6 HF5 and earlier.

Recommendations

CERT-EU recommends to upgrade to SolarWinds Platform 2022.4 [2].

References

[1] https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2022-4_release_notes.htm

[2] https://www.solarwinds.com/trust-center/security-advisories/cve-2022-36962