Blind SQL Injection Vulnerability (CVE-2021-35212)

Security Advisory Summary

An SQL injection Privilege Escalation Vulnerability was discovered in the Orion Platform reported by the ZDI Team. A blind Boolean SQL injection which could lead to full read/write over the Orion database content including the Orion certificate for any authenticated user.

Affected Products

- Orion 2019.2
- Orion 2019.4
- Orion 2020.2.1
- Orion 2020.2.4
- Orion 2020.2.5

Fixed Software Release

- Orion 2020.2.5 HF1
- Orion 2020.2.6
- Orion 2019.4.2
- Orion 2019.2 HF4

Acknowledgments

- Chudy working with Trend Micro Zero Day Initiative

Advisory Details

Severity

8.9 High

Advisory ID

CVE-2021-35212

First Published

07/15/2021

Fixed Version

Orion Platform 2020.2.5 HF1, 2020.2.6, 2019.4.2, 2019.2 HF4

CVSS Score

CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L