Deserialization of Untrusted Data Privilege Escalation Vulnerability (CVE-2021-27277)

Security Advisory Summary

This vulnerability allows local attackers to escalate privileges on affected installations of SolarWinds Orion Virtual Infrastructure Monitor 2020.2. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. The specific flaw exists within the OneTimeJobSchedulerEventsService WCF service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was formerly labeled ZDI-CAN-11955.

Advisory Details

Severity
8.8 High

Advisory ID
CVE-2021-27277

First Published
03/25/21

First Published
04/14/21

Version
SAM 2020.2.5

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

Affected Products

- Server & Application Monitor (SAM) versions 2020.2.4 and earlier

Fixed Software Release

- Server & Application Monitor (SAM) 2020.2.5

Acknowledgments

- Harrison Neal, ZDI Trend Micro