Deserialization of Untrusted Data Privilege Escalation Vulnerability (CVE-2021-27240)

Summary

This vulnerability allows local attackers to escalate privileges on affected installations of SolarWinds Patch Manager 2020.2.1. 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 DataGridService 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 Administrator. Was formerly labeled ZDI-CAN-12009.

Affected Products

- Patch Manager 2020.2.1 and earlier

Fixed Software Release

- Patch Manager 2020.2.1 HF 1

Acknowledgments

- Trend Micro, Zero Day Initiative

Advisory Details

Severity

8.7 High

Advisory ID

CVE-2021-27240

First Published

12/15/2020

Fixed Version

Patch Manager 2020.2.1 HF 1

CVSS Score

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