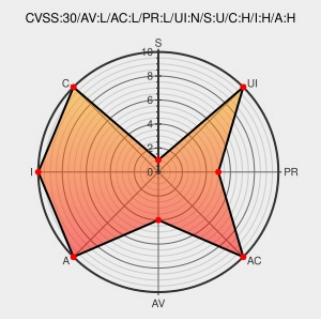
CVE-2021-27240

Published on: 03/29/2021 12:00:00 AM UTC

Last Modified on: 04/01/2021 07:02:00 PM UTC

CVE-2021-27240

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Patch Manager from Solarwinds contain the following vulnerability:

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 in order 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 ZDI-CAN-12009.

CVE-2021-27240 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SolarWinds** - **Patch Manager** version **2020.2.1**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
ZDI-21-207 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-207/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	Patch Manager	2020.2.1	All	All	All

cpe:2.3:a:solarwinds:patch_manager:2020.2.1:*:*:*:*:*:*:*

Discovery Credit

Harrison Neal

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→