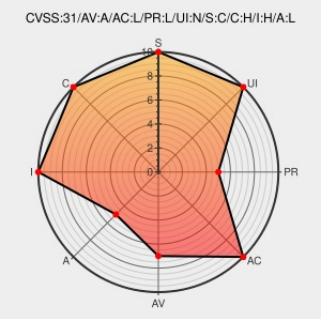
CVE-2021-35217

Published on: 09/08/2021 12:00:00 AM UTC

Last Modified on: 11/03/2021 08:22:00 PM UTC

CVE-2021-35217

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



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

Insecure Deseralization of untrusted data remote code execution vulnerability was discovered in Patch Manager Orion Platform Integration module and reported to us by ZDI. An Authenticated Attacker could exploit it by executing WSAsyncExecuteTasks deserialization of untrusted data.

CVE-2021-35217 has been assigned by psirt@solarwinds.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SolarWinds** - **Orion Platform** version **< 2020.2.6**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Success	support.solarwinds.com	CONFIRM support.solarwinds.com/SuccessCenter/s/article/Patch-Manager-2020-2-6-Hotfi

Center	text/html	Notes?language=en_US
Orion Platform 2020.2.6 Release Notes	documentation.solarwinds.com text/html	MISC documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/orion_p 2-6_release_notes.htm
Secure Configuration for the Orion Platform	documentation.solarwinds.com text/html	MISC documentation.solarwinds.com/en/success_center/orionplatform/content/core-secure configuration.htm
SolarWinds Trust Center Security Advisories | CVE-2021-35217	www.solarwinds.com text/html	MISC www.solarwinds.com/trust-center/security-advisories/cve-2021-35217
ZDI-21-1247 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-1247/

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	All	All	All	All

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

Discovery Credit

Jangggggg working with Trend Micro Zero Day Initiative

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-35217 : Insecure Deseralization of untrusted data remote code execution vulnerability was discovered in Pa… twitter.com/i/web/status/1…	2021-09-08 14:31:15

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report