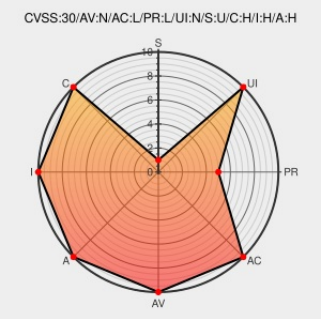
CVE-2021-31475

Published on: 05/21/2021 12:00:00 AM UTC

Last Modified on: 06/03/2021 06:03:00 PM UTC

CVE-2021-31475

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



Certain versions of Orion Job Scheduler from Solarwinds contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Orion Job Scheduler 2020.2.1 HF 2. Authentication is required to exploit this vulnerability. The specific flaw exists within the JobRouterService WCF service. The issue is due to the WCF service configuration, which allows a critical resource to be accessed by unprivileged users. An attacker can leverage this vulnerability to execute code in the context of an administrator. Was ZDI-CAN-12007.

CVE-2021-31475 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SolarWinds** - **Orion Job Scheduler** version **2020.2.1 HF 2**

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: 9 - HIGH

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

CVE References

Description	Tags	Link
Orion Platform 2020.2.5 Release Notes	documentation.solarwinds.com text/html	MISC documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/orion_p2-5_release_notes.htm
ZDI-21-605 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-605/

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.

Related QID Numbers

375655 SolarWinds Orion Job Scheduler Remote Code Execution Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	Orion Job Scheduler	2020.2.1	hotfix2	All	All

cpe:2.3:a:solarwinds:orion_job_scheduler:2020.2.1:hotfix2:*:*:*:*:*:*:

Discovery Credit

Harrison Neal

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31475 : This vulnerability allows remote attackers to execute arbitrary code on affected installations of… twitter.com/i/web/status/1…	2021-05-21 14:42:54
/r/netcve	CVE-2021-31475	2021-05-21 15:41:35

← Previous ID

Next ID→