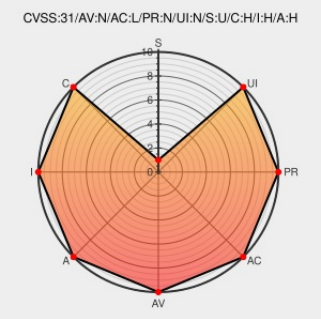
CVE-2020-10148

Published on: 12/29/2020 12:00:00 AM UTC

Last Modified on: 10/21/2022 05:17:00 PM UTC

CVE-2020-10148

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



Certain versions of Orion Platform from Solarwinds contain the following vulnerability:

The SolarWinds Orion API is vulnerable to an authentication bypass that could allow a remote attacker to execute API commands. This vulnerability could allow a remote attacker to bypass authentication and execute API commands which may result in a compromise of the SolarWinds instance. SolarWinds Orion Platform versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1 are affected.

CVE-2020-10148 has been assigned by cert@cert.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **SolarWinds** - **Orion Platform** version **= 2019.4 HF 5**

Affected Vendor/Software: **SolarWinds** - **Orion Platform** version **= 2020.2 without hotfix**

Affected Vendor/Software: **SolarWinds** - **Orion Platform** version **= 2020.2 HF 1**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisory | SolarWinds	Vendor Advisory www.solarwinds.com text/html	CONFIRM www.solarwinds.com/securityadvisory
VU#843464 - SolarWinds Orion API authentication bypass allows remote comand execution	Third Party Advisory US Government Resource kb.cert.org text/html	CERT-VN VU#843464

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

730169 Solarwinds Orion SUPERNOVA Malware Detected (Remote Detection)

Exploit/POC from Github

SolarWinds Orion API 远程代码执行漏洞批量检测脚本

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	Orion Platform	2019.4	hotfix5	All	All
Application	Solarwinds	Orion Platform	2020.2	-	All	All
Application	Solarwinds	Orion Platform	2020.2.1	hotfix1	All	All
Application	Solarwinds	Orion Platform	2019.4	hotfix5	All	All
Application	Solarwinds	Orion Platform	2020.2	-	All	All
Application	Solarwinds	Orion Platform	2020.2.1	hotfix1	All	All

cpe:2.3:a:solarwinds:orion_platform:2019.4:hotfix5:*:*:*:*:*:*:

cpe:2.3:a:solarwinds:orion_platform:2020.2:-:*:*:*:*:*:*:

cpe:2.3:a:solarwinds:orion_platform:2020.2.1:hotfix1:*:*:*:*:*:*:

cpe:2.3:a:solarwinds:orion_platform:2019.4:hotfix5:*:*:*:*:*:*:

cpe:2.3:a:solarwinds:orion_platform:2020.2:-:*:*:*:*:*:*:

cpe:2.3:a:solarwinds:orion_platform:2020.2.1:hotfix1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@UtopianKnightUK	Instead, they installed the malware on servers running Orion by exploiting CVE-2020-10148. Once installed, the atta… twitter.com/i/web/status/1…	2021-04-23 00:54:21
@campuscodi	CVE-2021-35211 (exploited in July) is the second SolarWinds zero-day exploited by hackers after CVE-2020-10148. Un… twitter.com/i/web/status/1…	2021-09-03 15:35:33
@ipssignatures	It's new to me that CheckPoint has a protection/signature/rule for the vulnerability CVE-2020-10148.... twitter.com/i/web/status/1…	2021-11-29 08:02:01
@ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-10148. ipssignatures.appspot.com/?cve=CVE-2020-… #S76u5qcvega2zs	2021-11-29 08:02:01
@RapidSafeguard	Saturday with #Shodan github.com/rdoix/CVE-2020… https://t.co/w8N6CHBmFu	2021-12-07 09:23:14

← Previous ID

Next ID→