

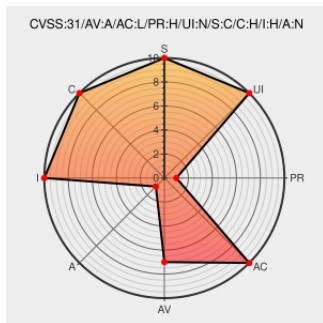


CVE-2021-35220

Published on: 08/31/2021 12:00:00 AM UTC

Last Modified on: 09/08/2021 06:25:00 PM UTC

CVE-2021-35220

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Orion Platform](#) from [Solarwinds](#) contain the following vulnerability:

Command Injection vulnerability in EmailWebPage API which can lead to a Remote Code Execution (RCE) from the Alerts Settings page.

CVE-2021-35220 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 HF1

Vulnerability Patch/Work Around

If you are unable to upgrade immediately. See SolarWinds Knowledgebase Article Below:
https://support.solarwinds.com/SuccessCenter/s/article/Mitigate-the-EmailWebPage-Command-Injection-RCE-CVE-2021-35220?language=en_US

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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
Page Not Found.	www.solarwinds.com text/html Inactive Link Not Archived	 MISC www.solarwinds.com/trust-center/security-advisories/cve-2021-35220
Success Center	support.solarwinds.com text/html	 MISC support.solarwinds.com/SuccessCenter/s/article/Orion-Platform-2020-2-6-Hotfix-1?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_p2-6_release_notes.htm
Success Center	support.solarwinds.com text/html	 MISC support.solarwinds.com/SuccessCenter/s/article/Mitigate-the-EmailWebPage-Command-Injection-RCE-CVE-2021-35220?language=en_US

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	Orion Platform	All	All	All	All
cpe:2.3:a:solarwinds:orion_platform:*:*:*:*:*.*						

Discovery Credit

SolarWinds would like to thank Alex Birnberg of Zymo Security and FireEye for reporting on the issue in a responsible manner.

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-35220 : Command Injection vulnerability in EmailWebPage API which can lead to a Remote Code Execution RCE... twitter.com/i/web/status/1...	2021-08-31 11:43:09
 @threatmeter	CVE-2021-35220 Command Injection vulnerability in EmailWebPage API which can lead to a Remote Code Execution (RCE)... twitter.com/i/web/status/1...	2021-09-01 07:10:40

[← Previous ID](#)

[Next ID →](#)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)