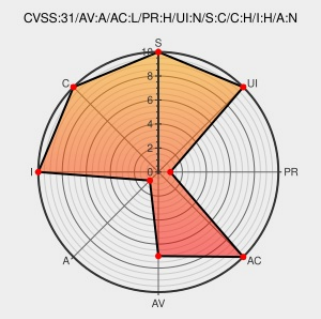
# CVE-2021-35220

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_p 2-6_release_notes.htm |
| Success Center | support.solarwinds.com text/html | MISC support.solarwinds.com/SuccessCenter/s/article/Mitigate-the-EmailWebPage-Comma RCE-CVE-2021-35220?language=en_US |



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→

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