

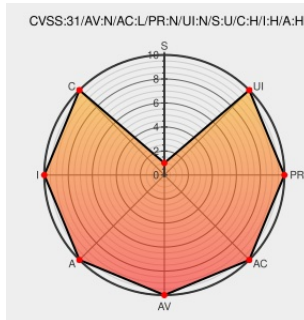


# CVE-2019-13551

Published on: 10/31/2019 12:00:00 AM UTC

Last Modified on: 05/13/2021 07:26:00 PM UTC

## CVE-2019-13551

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

Certain versions of [Wise-paas/rmm](#) from [Advantech](#) contain the following vulnerability:

Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. Path traversal vulnerabilities are caused by a lack of proper validation of a user-supplied path prior to use in file operations. An attacker can leverage these vulnerabilities to remotely execute code while posing as an administrator.

CVE-2019-13551 has been assigned by [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **10 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                      | Tags                                                                                                           | Link                                                                                                                                           |
|----------------------------------|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| ZDI-19-950   Zero Day Initiative | <a href="#">Third Party Advisory</a><br><a href="#">www.zerodayinitiative.com</a><br><a href="#">text/html</a> | <a href="#">Z</a> MISC <a href="https://www.zerodayinitiative.com/advisories/ZDI-19-950/">www.zerodayinitiative.com/advisories/ZDI-19-950/</a> |

|                                  |                                                                                                                                                                              |                                                                                                                                                         |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| ZDI-19-935   Zero Day Initiative | <a href="#">Third Party Advisory</a><br><a href="#">www.zerodayinitiative.com</a><br><a href="#">text/html</a>                                                               |  MISC <a href="#">www.zerodayinitiative.com/advisories/ZDI-19-935/</a>  |
| Advantech WISE-PaaS/RMM   CISA   | <a href="#">Mitigation</a><br><a href="#">Third Party Advisory</a><br><a href="#">US Government Resource</a><br><a href="#">www.us-cert.gov</a><br><a href="#">text/html</a> |  MISC <a href="#">www.us-cert.gov/ics/advisories/icsa-19-304-01</a>    |
| ZDI-19-958   Zero Day Initiative | <a href="#">Third Party Advisory</a><br><a href="#">www.zerodayinitiative.com</a><br><a href="#">text/html</a>                                                               |  MISC <a href="#">www.zerodayinitiative.com/advisories/ZDI-19-958/</a> |
| ZDI-19-941   Zero Day Initiative | <a href="#">Third Party Advisory</a><br><a href="#">www.zerodayinitiative.com</a><br><a href="#">text/html</a>                                                               |  MISC <a href="#">www.zerodayinitiative.com/advisories/ZDI-19-941/</a> |

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](mailto: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                                                  | <a href="#">Advantech</a> | <a href="#">Wise-paas/rmm</a> | All     | All    | All     | All      |
| Application                                                  | <a href="#">Advantech</a> | <a href="#">Wise-paas/rmm</a> | All     | All    | All     | All      |
| Application                                                  | <a href="#">Advantech</a> | <a href="#">Wise-pass/rmm</a> | All     | All    | All     | All      |
| Application                                                  | <a href="#">Advantech</a> | <a href="#">Wise-pass/rmm</a> | All     | All    | All     | All      |
| <a href="#">cpe:2.3:a:advantech:wise-paas\rmm:*:*:*:*:*:</a> |                           |                               |         |        |         |          |
| <a href="#">cpe:2.3:a:advantech:wise-paas\rmm:*:*:*:*:*:</a> |                           |                               |         |        |         |          |
| <a href="#">cpe:2.3:a:advantech:wise-pass\rmm:*:*:*:*:*:</a> |                           |                               |         |        |         |          |
| <a href="#">cpe:2.3:a:advantech:wise-pass\rmm:*:*:*:*:*:</a> |                           |                               |         |        |         |          |

No vendor comments have been submitted for this CVE

Social Mentions

| Source                                                        | Title | Posted (UTC) |
|---------------------------------------------------------------|-------|--------------|
| <div><a href="#">← Previous ID</a><span>Next ID→</span></div> |       |              |

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](#)