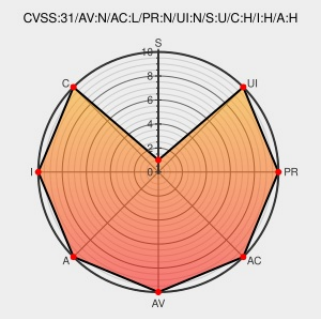
CVE-2019-13551

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 to track the vulnerability - currently rated as CRITICAL severity.

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: 10 - HIGH

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

CVE References

Description	Tags	Link
ZDI-19-950 | Zero Day Initiative	Third Party Advisory www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-19-950/

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advantech	Wise-paas/rmm	All	All	All	All
Application	Advantech	Wise-paas/rmm	All	All	All	All
Application	Advantech	Wise-pass/rmm	All	All	All	All
Application	Advantech	Wise-pass/rmm	All	All	All	All

cpe:2.3:a:advantech:wise-paas\/rmm:*:*:*:*:*:*:*:*:

cpe:2.3:a:advantech:wise-paas\/rmm:*:*:*:*:*:*:*:*:

cpe:2.3:a:advantech:wise-pass/rmm:*:*:*:*:*:*:*:*:

cpe:2.3:a:advantech:wise-pass\/rmm:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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