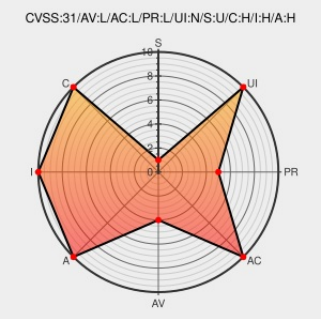
CVE-2021-38648

Published on: 09/15/2021 12:00:00 AM UTC

Last Modified on: 09/26/2021 09:25:00 PM UTC

CVE-2021-38648

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Azure Automation State Configuration from Microsoft contain the following vulnerability:

Open Management Infrastructure Elevation of Privilege Vulnerability
This CVE ID is unique from CVE-2021-38645, CVE-2021-38649.

CVE-2021-38648 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Microsoft** - **Azure Open Management Infrastructure** version

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
Security Update Guide - Microsoft Security Response Center	portal.msrc.microsoft.com text/html	MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38648

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

375860 Azure Open Management Infrastructure Multiple Vulnerabilities

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Azure Automation State Configuration	-	All	All	All
Application	Microsoft	Azure Automation Update Management	-	All	All	All
Application	Microsoft	Azure Diagnostics Lad	-	All	All	All
Application	Microsoft	Azure Open Management Infrastructure	-	All	All	All
Application	Microsoft	Azure Security Center	-	All	All	All
Application	Microsoft	Azure Sentinel	-	All	All	All
Application	Microsoft	Azure Stack Hub	-	All	All	All
Application	Microsoft	Container Monitoring Solution	-	All	All	All
Application	Microsoft	Log Analytics Agent	-	All	All	All
Application	Microsoft	System Center Operations Manager	-	All	All	All

cpe:2.3:a:microsoft:azure_automation_state_configuration:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:azure_automation_update_management:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:azure_diagnostics_\(lad\):-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:azure_open_management_infrastructure:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:azure_security_center:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:azure_sentinel:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:azure_stack_hub:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:container_monitoring_solution:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:log_analytics_agent:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:system_center_operations_manager:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

@autumn_good_35	CVE-2021-38647 CVE-2021-38648 CVE-2021-38645 CVE-2021-38649 OMIGOD: Critical Vulnerabilities in OMI Affecting Count… twitter.com/i/web/status/1…	2021-09-15 13:09:38
@0x009AD6_810	9月のPatch Tuesdayで修正されたAzure上のLinux VMに自動デプロイされるOMIエージェントの一連の脆弱性 (OMIGOD) CVE-2021-38647 root RCE CVE-2021-38648 EoP… twitter.com/i/web/status/1…	2021-09-15 16:19:54
@MrR0b0t18	CVE-2021-38647 CVE-2021-38648 CVE-2021-38645 CVE-2021-38649 Or Google OMIGOD	2021-09-15 22:54:20
@Root314	Threat Brief: OMI Vulnerabilities (CVE-2021-38645, CVE-2021-38647, CVE-2021-38648 and CVE-2021-38649)… twitter.com/i/web/status/1…	2021-09-16 19:09:38
@FINSIN_CL	"Unit42 Blog": Threat Brief: OMI Vulnerabilities (CVE-2021-38645, CVE-2021-38647, CVE-2021-38648 and CVE-2021-38649… twitter.com/i/web/status/1…	2021-09-16 19:15:24
@NaveedHamid	Threat Brief: OMI Vulnerabilities (CVE-2021-38645, CVE-2021-38647, CVE-2021-38648 and CVE-2021-38649) ift.tt/3kfbcsQ #cybersecurity	2021-09-16 19:16:29
@CyberIQs_	cyberiqs.com/threat-brief-o… #infosec #infosecurity #cybersecurity #threatintel #threatintelligence #hacking #cybernews… twitter.com/i/web/status/1…	2021-09-16 19:51:53
@PVynckier	Threat Brief: OMI Vulnerabilities (CVE-2021-38645, CVE-2021-38647, CVE-2021-38648 and CVE-2021-38649) unit42.paloaltonetworks.com/omi-vulnerabil…	2021-09-17 04:30:44
@NcuIsao	Threat Brief: OMI Vulnerabilities (CVE-2021-38645, CVE-2021-38647, CVE-2021-38648 and CVE-2021-38649)… twitter.com/i/web/status/1…	2021-09-17 15:56:11
@Securityblog	Threat Brief: OMI Vulnerabilities (CVE-2021-38645, CVE-2021-38647, CVE-2021-38648 and CVE-2021-38649) unit42.paloaltonetworks.com/omi-vulnerabil…	2021-09-18 11:28:46
/r/cybersecurity	Over 90 vulnerabilities in September updates. OMIGOD CVE-2021-38647, CVE-2021-38648, CVE-2021-38645, CVE-2021-38649	2021-09-14 18:22:18
/r/ciso	Over 90 vulnerabilities in September updates. OMIGOD CVE-2021-38647, CVE-2021-38648, CVE-2021-38645, CVE-2021-38649	2021-09-14 18:21:43
/r/sysadmin	“Secret” Agent Exposes Azure Customers To Unauthorized Code Execution	2021-09-15 23:42:13

← Previous ID

Next ID→