Security response

Learn more about Omnissa's external security vulnerability response policies and view Omnissa Security Advisories (OMSAs)

Omnissa external vulnerability response & remediation policy

We understand that unless our products adhere to the utmost standards for security, customers will lack the confidence to use them. To achieve this, Omnissa maintains a program to identify, respond, and manage vulnerabilities. This

How to report vulnerabilities

If you discover a vulnerability in an Omnissa product or service, kindly inform us by sending a confidential email to security@omnissa.com. Omnissa follows responsible vulnerability disclosure protocols, where researchers report newly identified vulnerabilities directly to us, allowing prompt mitigation before public disclosure, and may receive acknowledgment for their efforts.

CONTACT US

Safe harbor

Engaging in activities consistent with this policy will be deemed authorized, and Omnissa will refrain from pursuing legal action against you. Should a third party initiate legal proceedings related to activities under this policy, we will endeavor to affirm your compliance.

Omnissa Security Advisory (OMSAs)

Omnissa discloses vulnerabilities in Ominssa Security Advisories. OMSAs will include:.

CVSS Scoring & Severity Rating
Affected Products/Services
Vulnerability Details
Remediation Information
Acknowledgements
References

Omnissa Security Advisories

○ View All   Severity ⌄

Search vulnerabilities

		0002	2024-11468
Moderate	6.8	OMSA-2024-0001	**Workspace ONE UEM: CVE-2024-22260**
Moderate	6.3	OMSA-2023-0027	**Workspace ONE Launcher: CVE-2023-34064**
High	8.8	OMSA-2023-0025	**Workspace ONE UEM Console: CVE-2023-20866**
Moderate	5.3	OMSA-2023-0017	**Horizon Server: CVE-2023-34037, CVE-2023-34038**
Moderate	6.1	OMSA-2023-0011	**Omnissa Access, Identity Manager: CVE-2023-20884**
Moderate	6.3	OMSA-2023-0006	**Workspace ONE Content: CVE-2023-20857**
High	5.3 - 7.2	OMSA-2022-0032	**Omnissa Access, Identity Manager: CVE-2022-31700, CVE-2022-31701**
Critical	4.2 - 9.8	OMSA-2022-0028	**Workspace ONE Assist: Multiple CVEs**

			Multiple CVEs
Critical	7.8 - 9.8	OMSA-2022-0014	**Omnissa Access, Identity Manager: CVE-2022-22972, CVE-2022-22973**
High	7.3	OMSA-2022-0012	**Horizon Agent: CVE-2022-22962, CVE-2022-22964**
Critical	5.3 - 9.8	OMSA-2022-0011	**Omnissa Access, Identity Manager: Multiple CVEs**
Moderate	6.6	OMSA-2022-0006	**Workspace ONE Boxer: CVE-2022-22944**
Moderate	4.0	OMSA-2022-0002	**Workstation and Horizon Client for Windows: CVE-2022-22938**
Moderate	5.5 - 6.6	OMSA-2021-0030	**Omnissa Access, Identity Manager: CVE-2021-22056, CVE-2021-22057**
Critical	9.1	OMSA-2021-0029	**Workspace ONE UEM console: CVE-2021-22054**
Critical	9.0 - 10.0	OMSA-2021-0028	**Response to Apache Log4j RCE: CVE-2021-**

Moderate	5.3	OMSA-2021-0017	**Workspace ONE UEM console: CVE-2021-22029**
High	3.7 - 8.6	OMSA-2021-0016	**Omnissa Access, Identity Manager: CVE-2021-22002, CVE-2021-22003**

1 2 3

Offerings

Omnissa Platform

Platform Services

Products

Resources

Blog

Partners

Security Response

Trust Center

User Portal

Company

About

News

Careers

Contact Us