CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-075

VMWare Critical Vulnerability

December 18, 2021 — v1.0

TLP:WHITE

History:

- *18/12/2021 — v1.0 – Initial publication*

Summary

On December 17th, VMWare updated its security advisory related to CVE-2021-44228, and CVE-2021-45046 affecting many of its products [1]. While these CVE affect the Java logging library log4j, all products using this library are vulnerable *at least* to Unauthenticated Remote Code Execution [2].

Technical Details

The vulnerability exists in the Java logging library log4j. An unauthenticated remote attacker might exploit this vulnerability by sending specially crafted content to the application to execute malicious code on the server [2].

Affected products and Fixed Release

Vulnerable Product	Fixed Release	Workaround
VMware Horizon	2111, 7.13.1, 7.10.3	YES
VMware vCenter Server 7.x, 6.7.x, 6.5.x	Pending	YES
VMware vCenter Server 6.7.x, 6.5.x	Pending	YES
VMware HCX 4.0.x, 4.1.x, 4.2.x	Pending	YES
VMware NSX-T Data Center 3.x, 2.x	Pending	YES
VMware Unified Access Gateway 21.x, 20.x, 3.x	2111.1	YES
VMware Workspace ONE Access 21.x, 20.10.x	KB87183	YES
VMware Identity Manager 3.3.x	KB87185	YES
VMware vRealize Operations 8.x	Patch Pending	YES
VMware vRealize Operations Cloud Proxy	Patch Pending	YES
VMware vRealize Automation 8.x	Patch Pending	YES
VMware vRealize Automation 7.6	Patch Pending	YES
VMware vRealize Lifecycle Manager 8.x	Patch Pending	YES
VMware Carbon Black Cloud Workload Appliance 1.x	1.1.2	YES
VMware Carbon Black EDR Server 7.6.0, 7.5.x, 7.4.x, 7.3.x	Patch Pending	YES
VMware Site Recovery Manager, vSphere Replication 8.5, 8.4, 8.3	8.5.0.2, 8.4.0.4, 8.3.1.5	YES
VMware Tanzu GemFire 9.10.x	9.10.13, 9.9.7	YES

Vulnerable Product	Fixed Release	Workaround
VMware Tanzu GemFire for VMs 1.14.x, 1.13.x, 1.10.x	1.14.2, 1.13.5, 1.12.4, 1.10.9	YES
VMware Tanzu Greenplum 6.x	Patch Pending	YES
VMware Tanzu Operations Manager 2.x	2.8.18, 2.9.25, 2.10.24	YES
VMware Tanzu Application Service for VMs 2.x	2.6.23, 2.7.44, 2.8.30, 2.9.30, 2.10.24, 2.11.12 and 2.12.5	YES
VMware Tanzu Kubernetes Grid Integrated Edition 1.x	Patch Pending	YES
VMware Tanzu Observability by Wavefront Nozzle 3.x, 2.x	3.0.4	Pending
Healthwatch for Tanzu Application Service 2.x	2.1.8	Pending
Healthwatch for Tanzu Application Service 1.x	1.8.7	Pending
Spring Cloud Services for VMware Tanzu 1.x, 2.x, 3.x	1.1.4, 1.0.19, 2.1.10, 3.1.27	Pending for 1.x
Spring Cloud Gateway for Kubernetes 1.x	1.0.7	Pending
API Portal for VMware Tanzu 1.x	1.0.8	Pending
Single Sign-On for VMware Tanzu Application Service 1.x	1.14.6	Pending
App Metrics 2.x	2.1.2	Pending
VMware vCenter Cloud Gateway 1.x	Pending	YES
VMware vRealize Orchestrator 7.6, 8.x	Pending	YES
VMware Cloud Foundation 4.x, 3.x	Pending	YES
VMware Workspace ONE Access Connector (VMware Identity Manager Connector) 21.08.0.1, 21.08, 20.10, 19.03.0.1	KB87184	YES
VMware Horizon DaaS	Pending	YES
VMware Horizon Cloud Connector 1.x, 2.x	2.1.2	Pending
VMware NSX Data Center for vSphere 6.x	Pending	YES
VMware AppDefense Appliance 2.x	N/A	YES
VMware Cloud Director Object Storage Extension 2.0.x, 2.1.x	2.0.0.3, 2.1.0.1	YES
VMware Telco Cloud Operations 1.x	Pending	YES
VMware vRealize Log Insight 8.2, 8.3, 8.4, 8.6	Pending	YES
VMware Tanzu Scheduler 1.x	1.6.1	YES
VMware Smart Assurance NCM 10.1.6	Pending	YES
VMware Smart Assurance SAM (Service Assurance Manager) 10.1.0.x, 10.1.2, 10.1.5,	Pending	YES
VMware Integrated OpenStack 7.x	Pending	YES
VMware vRealize Business for Cloud 7.x	Pending	YES
VMware vRealize Network Insight 5.3, 6.x	Pending	YES
VMware Cloud Provider Lifecycle Manager 1.x	1.2.0.1	YES
VMware SD-WAN VCO 4.x	Pending	YES
VMware NSX-T Intelligence Appliance 1.2.x, 1.1.x	Pending	YES
VMware Horizon Agents Installer 21.x.x, 20.x.x	KB87157	YES
VMware Tanzu Observability Proxy 10.x	10.12	YES

Recommendations

CERT-EU recommends applying the patches, or upgrading the products as soon as possible. Refer to the table in Affected products and Fixed Release section and to details provided by CISCO in [1] to find the fixed release of each product.

References

[1] https://www.vmware.com/security/advisories/VMSA-2021-0028.html

[2] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf