Hive Pro

THREAT ADVISORY

Drop everything and patch VMware's vCenter Server Vulnerabilities

TA202136

Threat Level GREEN

Publish Date – Sept 22, 2021

VMware has issued patches for 19 new vulnerabilities. CVE-2021-22005 is the worst of the lot, defined as "an arbitrary file upload vulnerability in the Analytics service" of the vCenter Server. An attacker with network access to vCenter Server's port 443 might use this flaw to execute code on the server by uploading a specially crafted file. VMware also provides a temporary workaround for individuals who are unable to instantly patch their appliances.

Vulnerability Details

CVE ID`	Affected Products	Affected CPE	Vulnerability Name
CVE-2021-22005	vCenter Server:7, 6.7(virtual app), Cloud Foundation (vCenter Server):4.x, 3.x	cpe:2.3:a:vmware:vcenter_server:6.7:-:*:*:*:*:*:* , cpe:2.3:a:vmware:vcenter_server:7.0:-:*:*:*:*:*:* , cpe:2.3:a:vmware:cloud_foundation:3.0:*:*:*:*:*:*:*, cpe:2.3:a:vmware:cloud_foundation:4.0:*:*:*:*:*:*:*	vCenter Server file upload vulnerability
CVE-2021-22007			vCenter Server local information disclosure vulnerability
CVE-2021-22010			vCenter Server VPXD denial of service vulnerability
CVE-2021-22020			vCenter Server Analytics service denial-of-service vulnerability
CVE-2021-22006	vCenter Server:7, 6.7, Cloud Foundation (vCenter Server):4.x, 3.x		vCenter Server reverse proxy bypass vulnerability
CVE-2021-22012	vCenter Server:6.5	cpe:2.3:a:vmware:vcenter_server:6.5:-:*:*:*:*:*:*	vCenter Server unauthenticated API information disclosure vulnerability
CVE-2021-22013			vCenter Server file path traversal vulnerability
CVE-2021-22016	vCenter Server:6.7	cpe:2.3:a:vmware:vcenter_server:6.7:-:*:*:*:*:*:*	vCenter Server reflected XSS vulnerability

Hive Pro

THREAT ADVISORY

CVE ID`	Affected Products	Affected CPE	Vulnerability Name
CVE-2021-21991	vCenter Server:7, 6.7, 6.5, Cloud Foundation (vCenter Server):4.x, 3.x	cpe:2.3:a:vmware:vcenter_server:6.5:-:*:*:*:*:*:* , cpe:2.3:a:vmware:vcenter_server:6.7:-:*:*:*:*:*:* , cpe:2.3:a:vmware:vcenter_server:7.0:-:*:*:*:*:*:* , cpe:2.3:a:vmware:cloud_foundation:3.0:*:*:*:*:*:*:*, cpe:2.3:a:vmware:cloud_foundation:4.0:*:*:*:*:*:*:*	vCenter Server local privilege escalation vulnerability
CVE-2021-22011			vCenter server unauthenticated API endpoint vulnerability
CVE-2021-22014			vCenter Server authenticated code execution vulnerability
CVE-2021-21992			vCenter Server XML parsing denial-of-service vulnerability
CVE-2021-22019			vCenter Server denial of service vulnerability
CVE-2021-22009			vCenter Server VAPI multiple denial of service vulnerabilities
CVE-2021-22008			vCenter Server information disclosure vulnerability
CVE-2021-21993			vCenter Server SSRF vulnerability
CVE-2021-22015			vCenter Server improper permission local privilege escalation vulnerabilities
CVE-2021-22017	vCenter Server:6.7, 6.5	cpe:2.3:a:vmware:vcenter_server:6.5:-:*:*:*:*:*:* , cpe:2.3:a:vmware:vcenter_server:6.7:-:*:*:*:*:*:*	vCenter Server rhttpproxy bypass vulnerability
CVE-2021-22018	vCenter Server:7, Cloud Foundation (vCenter Server):4.x	cpe:2.3:a:vmware:vcenter_server:7.0:-:*:*:*:*:*:* , cpe:2.3:a:vmware:cloud_foundation:4.0:*:*:*:*:*:*:*	vCenter Server file deletion vulnerability

Patch Link

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

References

https://blogs.vmware.com/vsphere/2021/09/vmsa-2021-0020-what-you-need-to-know.html
https://www.theregister.com/2021/09/22/vmware_emergency_vcenter_patch_recommendation/