TLP: WHITE

Advisory Alert

Alert Number : AAA20201204 **Date :** December 4, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	High	Command Injection Vulnerability
HP	High	Multiple Remote Vulnerabilities
Apache	High	Information disclosure vulnerability

Description

Affected Product	VMware
Severity	High
Affected Vulnerability	Command Injection Vulnerability (CVE-2020-4006)
Description	Vmware has released security patch update addressing command injection vulnerability that was identified in multiple products. An attacker with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account can execute commands with unrestricted privileges on the underlying operating system. This account is internal to the impacted products and a password is set at the time of deployment. In order to exploit this vulnerability the malicious actor must possess this password.
Affected Products	VMware Workspace One Access (Access) VMware Workspace One Access Connector (Access Connector) VMware Identity Manager (vIDM) VMware Identity Manager Connector (vIDM Connector) VMware Cloud Foundation vRealize Suite Lifecycle Manager
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0027.html

Affected Product	HP
Severity	High
Affected Vulnerability	Multiple Remote Vulnerabilities
Description	HP has released security patch updates addressing multiple vulnerabilities that were identified in HPE HP-UX Web Server Suite running Apache on HP-UX 11iv3. These vulnerabilities include remote code execution, denial of service, bypass access control restrictions, disclose sensitive information, add or modify data, memory corruption, or redirection of a URL to an untrusted URL.
Affected Products	HP-UX Web Server Suite Software - HP-UX Apache-based Web Server v.2.4.18.05 and earlier.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04050en_us

Affected Product	Apache
Severity	High
Affected Vulnerability	Information disclosure vulnerability (CVE-2020-17527)
Description	Apache has released security patch updates addressing vulnerability that exists in their products. By exploiting this vulnerability a remote attacker can trigger sensitive information disclosure on the targeted systems.
Affected Products	Apache Tomcat 10.0.0-M1 – 10.0.0-M9 Apache Tomcat 9.0.0.M5 – 9.0.39 Apache Tomcat 8.5.1 - 8.5.59
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	http://tomcat.apache.org/security-10.html http://tomcat.apache.org/security-9.html http://tomcat.apache.org/security-8.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.