Advisory Alert

Alert Number: **AAA20220217** **Date:** **February 17, 2022**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple vulnerabilities
Cisco	**High**	Multiple vulnerabilities
Drupal	**High**	Multiple vulnerabilities

Description

Affected Product	VMware
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-22945, CVE-2021-22040, CVE-2021-22041, CVE-2021-22042, CVE-2021-22043, CVE-2021-22050)
Description	VMware has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2022-22945** - A malicious actor with SSH access to an NSX-Edge appliance (NSX-V) can execute arbitrary commands on the operating system as root. **CVE-2021-22040** - VMware ESXi, Workstation, and Fusion contain a use after free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE-2021-22041** - VMware ESXi, Workstation, and Fusion contain a double-fetch vulnerability in the UHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE-2021-22042** - VMware ESXi contains an unauthorized access vulnerability due to VMX having access to settingsd authorization tickets. A malicious actor with privileges within the VMX process only, may be able to access settingsd service running as a high privileged user. **CVE-2021-22043** - VMware ESXi contains a TOCTOU (Time-of-check Time-of-use) vulnerability that exists in the way temporary files are handled. A malicious actor with access to settingsd, may exploit this issue to escalate their privileges by writing arbitrary files. **CVE-2021-22050** - ESXi contains a slow HTTP POST denial-of-service vulnerability in rhttpproxy. A malicious actor with network access to ESXi may exploit this issue to create a denial-of-service condition by overwhelming rhttpproxy service with multiple requests.
Affected Products	VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware Cloud Foundation (Cloud Foundation) VMware NSX Data Center for vSphere (NSX-V)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0004.html https://www.vmware.com/security/advisories/VMSA-2022-0005.html

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20659, CVE-2022-20750, CVE-2022-20653)
Description	Cisco has released Security Updates addressing for multiple vulnerabilities. **CVE-2022-20659 -** The vulnerability exists due to insufficient sanitization of user-supplied data in the web-based management interface. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website**.** **CVE-2022-20750 -** The vulnerability exists due to improper input validation of an ingress TCP packets. A remote attacker can send a specially crafted TCP traffic to the affected system and cause the checkpoint manager process to restart. **CVE-2022-20653 -** A vulnerability in the DNS-based Authentication of Named Entities email verification component of Cisco AsyncOS Software for Cisco Email Security Appliance could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device.
Affected Products	Cisco Prime Infrastructure and Cisco EPN Manager. Cisco RCM for Cisco StarOS Software. Cisco ESA
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-xss-P8fBz2FW https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-tcp-dos-2Wh8XjAQ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-MxZvGtgU

Affected Product	Drupal
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-25270, CVE-2022-25271)
Description	Drupal has released Security Updates addressing for multiple vulnerabilities. **CVE-2022-25270 -** The Quick Edit module does not properly check entity access in some circumstances. This could result in users with the access in place editing permission viewing some content they are are not authorized to access. **CVE-2022-25271 -** Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.
Affected Products	Drupal 9.3, update to Drupal 9.3.6. Drupal 9.2, update to Drupal 9.2.13. Drupal 7, update to Drupal 7.88.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-004 https://www.drupal.org/sa-core-2022-003

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.