Advisory Alert

Alert Number: AAA20210825 **Date:** August 25, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**High**	Multiple Vulnerabilities
Joomla	**High**	Privilege Escalation Vulnerability
OpenSSL	**High**	Multiple Vulnerabilities

Description

Affected Product	VMware
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22022, CVE-2021-22023, CVE-2021-22024, CVE-2021-22025, CVE-2021-22026, CVE-2021-22027)
Description	VMWare has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2021-22022, CVE-2021-22023** - A malicious user with administrative access to the vRealize Operations Manager API can read any file on the server that causes information disclosure & modify other users information leading to an account takeover. **CVE-2021-22024, CVE-2021-22025 -** An unauthenticated malicious user with network access to the vRealize Operations Manager API can read any log file resulting in sensitive information disclosure and it's allowed to add new nodes to existing vROps cluster. **CVE-2021-22026, CVE-2021-22027 –** An unauthenticated malicious actors with network access to the vRealize Operations Manager API can perform server-side request spoofing attacks leading to information disclosure.
Affected Products	VMware vRealize Operations 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-2021-0018.html

Affected Product	Joomla
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2021-26040)
Description	Joomla has released a security patch update addressing Privilege Escalation vulnerabilities that exist in their product.The media manager does not correctly check the user's permissions before executing a file deletion command. Joomla recommends to upgrade the joomla versions in to version 4.0.1 in order to avoid issues with below mentioned versions.
Affected Products	Joomla CMS versions 4.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

Affected Product	OpenSSL
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3711,CVE-2021-3712)
Description	**CVE-2021-3711** - The vulnerability exists due to a boundary error in EVP_PKEY_decrypt() function within implementation of the SM2 decryption. A remote attacker can send specially crafted SM2 content for decryption to trigger a buffer overflow by 62 bytes and execute arbitrary code on the target system **CVE-2021-3712** - The vulnerability exists due to a boundary condition when processing ASN.1 strings related to a confusion with NULL termination of strings in array. A remote attacker can pass specially crafted data to the application to trigger an out-of-bounds read error and read contents of memory on the system or perform a denial of service.
Affected Products	OpenSSL versions 1.1.1k and below are affected by this issue
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20210824.txt

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.