Advisory Alert

Alert Number : AAA20220324 **Date :** March 24, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	**Multiple Vulnerabilities**
Drupal	**Critical**	**Third-party libraries Vulnerability**

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22951, CVE-2022-22952)
Description	**CVE-2022-22951 -** VMware Carbon Black App Control contains an OS command injection vulnerability. An authenticated, high privileged malicious actor with network access to the VMware App Control administration interface may be able to execute commands on the server due to improper input validation leading to remote code execution. **CVE-2022-22952 -** VMware Carbon Black App Control contains a file upload vulnerability. A malicious actor with administrative access to the VMware App Control administration interface may be able to execute code on the Windows instance where AppC Server is installed by uploading a specially crafted file.
Affected Products	VMware Carbon Black App Control (AppC)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0008.html

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Third-party libraries Vulnerability (CVE-2022-24775)
Description	Drupal has patched a Guzzle third-party library vulnerability that affects multiple versions of Drupal Core. The Guzzle library is used for handling HTTP requests and responses to external services. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values.
Affected Products	Drupal 9.3, update to Drupal 9.3.9. Drupal 9.2, update to Drupal 9.2.16.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-006

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.