Advisory Alert

Alert Number: AAA20230316 **Date:** March 16, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Medium**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities can leads to information disclosure, and access bypass. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Drupal 7, 9.4, 9.5 and 10.0 Drupal Media Responsive Thumbnail module versions prior to 8.x-1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2023-002 https://www.drupal.org/sa-core-2023-003 https://www.drupal.org/sa-core-2023-004 https://www.drupal.org/sa-contrib-2023-010

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21198, CVE-2022-28624)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-21198 -** Time-of-check time-of-use race condition in the BIOS firmware for some Intel Processors that uses in HPE products may allow a privileged user to potentially enable privilege escalation via local access. **CVE-2022-28624 –** A vulnerability exist in certain HPE FlexNetwork and FlexFabric switch products that could be remotely exploited to allow cross site scripting (XSS). HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE FlexFabric 5700 Switch Series - Prior to R2432P61 HPE FlexFabric 5710 Switch Series - Prior to R6710 HPE FlexFabric 5930 Switch Series - Prior to R2432P61 HPE FlexFabric 5940 Switch Series - Prior to R6710 HPE FlexFabric 5945 Switch Series - Prior to R6710 HPE FlexNetwork 5130 EI Switch Series - Prior to R3507P08 HPE FlexNetwork 10500 Switch Series - Prior to R7634P09 HPE ProLiant m510 Server Cartridge -Prior to 1.96_10-13-2022 HPE ProLiant DL20 Gen10 Plus server - Prior to 1.64_10-20-2022 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to 1.64_10-20-2022 HPE ProLiant ML30 Gen10 Plus server - Prior to 1.64_10-20-2022
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04380en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04379en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04265en_us

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.