# Advisory Alert

**Alert Number:** AAA20230922 **Date:** September 22, 2023

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Drupal** | **Critical** | Cache Poisoning vulnerability |
| **HPE** | **High, Medium** | Multiple vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Drupal** |
| Severity | **Critical** |
| Affected Vulnerability | Cache Poisoning vulnerability |
| Description | Drupal has released a critical security update addressing a Cache Poisoning vulnerability affecting certain versions of Drupal core.<br>In specific scenarios, Drupal's JSON:API module may output error backtraces, potentially causing sensitive information to be cached and accessible to anonymous users. This could result in privilege escalation.<br>Drupal recommends to apply the necessary security updates at earliest to avoid issues. |
| Affected Products | Drupal 8.7.0 to 9.5.11<br>Drupal 10.0 to 10.0.11<br>Drupal 10.1 to 10.1.4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.drupal.org/sa-core-2023-006 |

| | |
|---|---|
| Affected Product | **HPE** |
| Severity | **High, Medium** |
| Affected Vulnerability | Multiple vulnerabilities (CVE-2022-21131, CVE-2022-21136, CVE-2022-21123, CVE-2022-21127, CVE-2022-21125, CVE-2022-21166, CVE-2023-20594, CVE-2023-20597) |
| Description | HPE has released security updates addressing multiple security vulnerabilities in certain products using Intel Xeon Processors, as well as potential security vulnerabilities in HPE ProLiant AMD XL Servers and HPE ProLiant AMD DL Servers.<br>These vulnerabilities could be exploited locally, resulting in various security risks, including disclosure of sensitive information and denial of service (DoS) in the case of HPE products.<br><br>HPE recommends to apply the necessary security updates at earliest to avoid issues. |
| Affected Products | HPE NonStop NS8 X4 CPU - Prior to 2.66_05-17-2022 - SPR T0918L02^AAR<br>HPE NonStop NS4 X4 CPU - Prior to 2.66_05-17-2022 - SPR T0918L02^AAR<br>HPE NonStop NS7 X3 CPU - Prior to 2.66_06-01-2022 - SPR T0918L02^AAR<br>HPE NonStop NS3 X3 CPU - Prior to 2.66_06-01-2022 - SPR T0918L02^AAR<br>HPE NonStop NS2 X3 - Prior to 2.66_05-17-2022 - SPR T0918L02^AAR<br>HPE NonStop Network CLIM Gen10 - Prior to 2.66_05-17-2022 - SPR T0848L02^ABL<br>HPE NonStop Storage CLIM Gen10 - Prior to 2.66_05-17-2022 - SPR T0848L02^ABL<br>HPE NonStop System Console (NSC) Gen10 - Prior to 2.66_05-17-2022 - SPR T0918L02^AAR<br>HPE NonStop Virtual Tape Controller (VTC) Gen10 - Prior to 2.66_05-17-2022 - SPR T0918L02^AAR<br>HPE NonStop Virtual Tape Repository (VTR) Gen10 - Prior to 2.66_05-17-2022 - SPR T0918L02^AAR<br>HPE Integrity NonStop BladeSystem NB56000c - Please refer to the entries for HPE NonStop Network and Storage CLIMs<br>HPE Integrity NonStop NS2400 - Please refer to the entries for HPE NonStop Storage CLIMs<br>HPE Integrity NonStop NS2300 - Please refer to the entries for HPE NonStop Storage CLIMs<br>HPE NonStop NS8 X4 CPU - Prior to 2.66_05-17-2022<br>HPE NonStop NS4 X4 CPU - Prior to 2.66_05-17-2022<br>HPE NonStop NS7 X3 CPU - Prior to 2.66_06-01-2022<br>HPE NonStop NS3 X3 CPU - Prior to 2.66_06-01-2022<br>HPE NonStop NS7 X2 CPU - Prior to 2.96_05-17-2022<br>HPE NonStop NS3 X2 CPU - Prior to 2.96_05-17-2022<br>HPE NonStop NS2 X3 - Prior to 2.66_05-17-2022<br>HPE NonStop NS2 X2 - Prior to 2.96_05-17-2022<br>HPE NonStop Network CLIM Gen10 - Prior to 2.66_05-17-2022<br>HPE NonStop Storage CLIM Gen10 - Prior to 2.66_05-17-2022<br>HPE NonStop System Console (NSC) Gen10 - Prior to 2.66_05-17-2022<br>HPE NonStop Virtual Tape Controller (VTC) Gen10 - Prior to 2.66_05-17-2022<br>HPE NonStop Virtual Tape Repository (VTR) Gen10 - Prior to 2.66_05-17-2022<br>HPE NonStop Network CLIM Gen9 - Prior to 2.96_05-17-2022<br>HPE NonStop Storage CLIM Gen9 - Prior to 2.96_05-17-2022<br>HPE NonStop System Console (NSC) Gen9 - Prior to 2.96_05-17-2022<br>HPE NonStop Virtual Tape Controller (VTC) Gen9 - Prior to 2.96_05-17-2022<br>HPE NonStop Virtual Tape Repository (VTR) Gen9 - Prior to 2.96_05-17-2022<br>HPE ProLiant XL675d Gen10 Plus Server - Prior to v2.64_11-30-2022<br>HPE ProLiant XL645d Gen10 Plus Server - Prior to v2.64_11-30-2022<br>HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v2.64_11-30-2022<br>HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v2.64_11-17-2022<br>HPE ProLiant DL345 Gen10 Plus server - Prior to v2.64_11-17-2022<br>HPE ProLiant DL365 Gen10 Plus server - Prior to v2.64_11-17-2022<br>HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v2.64_11-17-2022 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbns04340en_us<br>https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbns04339en_us<br>https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04541en_us<br>https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04537en_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.**