



Advisory Alert

Alert Number: AAA20231221

Date: December 21, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	High	Multiple Vulnerabilities
Apache Guacamole	High	Integer Overflow Vulnerability
IBM	Medium	Denial of Service Vulnerability

Description

Affected Product	HPE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-50273)
Description	HPE has released security updates addressing multiple vulnerabilities in HPE Unified OSS Console (UOC). These vulnerabilities could be exploited to allow local cross-site scripting, and local/remote denial of service. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE Unified OSS Console (UOC) - Prior to Version 3.0.47
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=hpesbmu04581en_us

Affected Product	Apache Guacamole
Severity	High
Affected Vulnerability	Integer overflow vulnerability (CVE-2023-43826)
Description	Apache Guacamole has released a security update addressing an Integer overflow vulnerability in their products. CVE-2023-43826 - Apache Guacamole 1.5.3 and older do not consistently ensure that values received from a VNC server will not result in integer overflow. If a user connects to a malicious or compromised VNC server, specially-crafted data could result in memory corruption, possibly allowing arbitrary code to be executed with the privileges of the running guacd process. Apache Guacamole recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Apache Guacamole prior to 1.5.4 version
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://guacamole.apache.org/security/

Affected Product	IBM
Severity	Medium
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-45165)
Description	IBM has released a security update addressing a Denial of Service vulnerability in their products. CVE-2023-45165 - A vulnerability in the AIX SMB client daemon could allow a non-privileged local user to cause a Denial of Service. AIX uses the SMB client daemon to access files on SMB servers. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM - AIX 7.2, 7.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7100970

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.