Advisory Alert

Alert Number: AAA20221116 **Date:** November 16, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Samba	**High**	Buffer Overflow Vulnerability
HP	**High**	Denial of Service Vulnerability
Redhat	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Samba**
Severity	**High**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2022-42898)
Description	Samba has released Security Updates addressing Buffer Overflow vulnerability that exist in their products. A remote user can send a specially crafted request to the Kerberos DC server, trigger an integer overflow, and execute arbitrary code on the target system. Samba recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	All versions of Samba prior to 4.15.12, 4.16.7, 4.17.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2022-42898.html

Affected Product	**HP**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2022-0778)
Description	HP has released Security Updates addressing Denial of Service Vulnerability that exist in their products. A potential security vulnerability has been identified in Integrated Lights-Out 5 (iLO 5), or Integrated Lights-Out 4 (iLO 4). The vulnerability could be remotely exploited to allow denial of service. HP recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - Prior to v2.72 HPE Integrated Lights-Out 4 (iLO 4) - Prior to v2.81 Multiple Models of HPE ProLiant DL, DX, ML,XL Series HPE Storage HPE StoreEasy HPE Apollo HPE StoreVirtual HPE Synergy HP ConvergedSystem
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04366en_us

Affected Product	**Redhat**
Severity	**High,** Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-25032, CVE-2021-46828, CVE-2022-1348, CVE-2021-25220, CVE-2022-37434, CVE-2020-36516, CVE-2021-3640, CVE-2022-0168, CVE-2022-0617, CVE-2022-0854, CVE-2022-1016, CVE-2022-1048, CVE-2022-1184, CVE-2022-1280, CVE-2022-1353, CVE-2022-1679, CVE-2022-1852, CVE-2022-1998, CVE-2022-2586, CVE-2022-2639, CVE-2022-20368, CVE-2022-21123, CVE-2022-21125, CVE-2022-21166, CVE-2022-21499, CVE-2022-23816, CVE-2022-23825, CVE-2022-24448, CVE-2022-26373, CVE-2022-28390, CVE-2022-28893, CVE-2022-29581, CVE-2022-29900, CVE-2022-29901, CVE-2022-36946, CVE-2022-39190, CVE-2021-3839, CVE-2022-2132, CVE-2022-28199, CVE-2022-24795, CVE-2022-1705, CVE-2022-30630, CVE-2022-30631, CVE-2022-30632, CVE-2022-30635, CVE-2022-32148, CVE-2022-2309, CVE-2022-2319, CVE-2022-2320, CVE-2022-1328, CVE-2022-30550, CVE-2021-21708, CVE-2022-31625, CVE-2022-0561, CVE-2022-0562, CVE-2022-0865, CVE-2022-0891, CVE-2022-0908, CVE-2022-0909, CVE-2022-0924, CVE-2022-1354, CVE-2022-1355, CVE-2022-22844, CVE-2022-0918, CVE-2022-0996, CVE-2022-2850, CVE-2022-27337, CVE-2022-1706, CVE-2022-26125, CVE-2021-0561, CVE-2022-0934, CVE-2022-0396, CVE-2022-22719, CVE-2022-22721, CVE-2022-23943, CVE-2022-26377, CVE-2022-28614, CVE-2022-28615, CVE-2022-29404, CVE-2022-30522, CVE-2022-30556, CVE-2022-31813, CVE-2022-30698, CVE-2022-30699, CVE-2021-23648, CVE-2022-1962, CVE-2022-21673, CVE-2022-21698, CVE-2022-21702, CVE-2022-21703, CVE-2022-21713, CVE-2022-28131, CVE-2022-30633, CVE-2022-22624, CVE-2022-22628, CVE-2022-22629, CVE-2022-22662, CVE-2022-26700, CVE-2022-26709, CVE-2022-26710, CVE-2022-26716, CVE-2022-26717, CVE-2022-26719, CVE-2022-30293, CVE-2022-25255, CVE-2022-25308, CVE-2022-25309, CVE-2022-25310, CVE-2021-20291, CVE-2021-33195, CVE-2021-33197, CVE-2021-33198, CVE-2022-2989, CVE-2022-2990, CVE-2022-27191, CVE-2022-30067, CVE-2022-32990, CVE-2021-22570, CVE-2020-28851, CVE-2020-28852 CVE-2021-4024, CVE-2021-20199, CVE-2021-34558)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit the most severe vulnerabilities to cause arbitrary code execution, information disclosure, privilege escalation, cache poisoning, heap-based buffer overflow. Redhat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:8194 https://access.redhat.com/errata/RHSA-2022:8162 https://access.redhat.com/errata/RHSA-2022:8151 https://access.redhat.com/errata/RHSA-2022:8126 https://access.redhat.com/errata/RHSA-2022:8112 https://access.redhat.com/errata/RHSA-2022:8098 https://access.redhat.com/errata/RHSA-2022:8078 https://access.redhat.com/errata/RHSA-2022:8070 https://access.redhat.com/errata/RHSA-2022:8068 https://access.redhat.com/errata/RHSA-2022:8067 https://access.redhat.com/errata/RHSA-2022:8062 https://access.redhat.com/errata/RHSA-2022:8057 https://access.redhat.com/errata/RHSA-2022:8054 https://access.redhat.com/errata/RHSA-2022:8022 https://access.redhat.com/errata/RHSA-2022:8011 https://access.redhat.com/errata/RHSA-2022:8008 https://access.redhat.com/errata/RHSA-2022:7978 https://access.redhat.com/errata/RHSA-2022:7970 https://access.redhat.com/errata/RHSA-2022:7954 https://access.redhat.com/errata/RHSA-2022:7933

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.