Advisory Alert

Alert Number: AAA20231004 **Date:** October 4, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	**High**	Denial-of-Service Vulnerability
HPE	**High**	Multiple Privilege Escalation Vulnerabilities
Redhat	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Palo Alto**
Severity	**High**
Affected Vulnerability	Denial-of-Service Vulnerability (CVE-2023-38802)
Description	Palo Alto has released a security update addressing Denial-of-Service Vulnerability exists due to insufficient validation of user-supplied input. A remote attacker can send specially crafted BGP update data to the application and perform a denial of service (DoS) attack Palo Alto recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	PAN-OS 11.0 version before 11.0.3 PAN-OS 10.2 version before 10.2.6 PAN-OS 10.1 version before 10.1.11 PAN-OS 9.1 version before 9.1.16-h3 Prisma SD-WAN ION 6.2 version before 6.2.3 Prisma SD-WAN ION 6.1 version before 6.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-38802

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Privilege Escalation Vulnerabilities (CVE-2022-26837, CVE-2021-0187, CVE-2022-32231, CVE-2022-26343, CVE-2022-30704)
Description	HPE has released a security update addressing Multiple Vulnerabilities exist in in their products. Successful exploitation of these vulnerabilities could lead to denial of service and information disclosure. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE ProLiant BL460c Gen10 Server Blade -prior to 2.76_02-09-2023 HPE ProLiant DL20 Gen10 Server -prior to 2.68_01-12-2023 HPE ProLiant DL160 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL180 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL360 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL380 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL560 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant ML110 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant ML30 Gen10 Server -prior to 2.68_01-12-2023 HPE ProLiant ML350 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL20 Gen10 Plus server -prior to 1.68_01-12-2023 HPE ProLiant DL110 Gen10 Plus Telco server -prior to 1.72_02-02-2023 HPE ProLiant DL360 Gen10 Plus server -prior to 1.72_02-02-2023 HPE ProLiant DL380 Gen10 Plus server -prior to 1.72_02-02-2023 HPE ProLiant MicroServer Gen10 Plus v2 -prior to 1.68_01-12-2023 HPE ProLiant ML30 Gen10 Plus server -prior to 1.68_01-12-2023 HPE ProLiant BL460c Gen9 Server Blade - Prior to 3.08_01-12-2023 HPE ProLiant BL480c Server Blade - Prior to 3.08_01-12-2023 HPE ProLiant BL660c Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant DL60 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant DL80 Gen9 Server - Prior to 3.08_01-12-2023 HP ProLiant DL120 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant DL160 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant DL180 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant DL360 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant DL380 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant DL560 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant ML110 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant ML150 Gen9 Server - Prior to 3.08_01-12-2023 HPE ProLiant ML350 Gen9 Server - Prior to 3.08_01-12-2023
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04414en_us

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32233, CVE-2023-20593, CVE-2023-35001)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to stack-out-of-bounds-reads, privilege escalation, and Cross-Process Information Leak. Redhat recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux Server - AUS 7.7 x86_64 Red Hat Enterprise Linux Server - AUS 7.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5414 https://access.redhat.com/errata/RHSA-2023:5419

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29256, CVE-2023-34455, CVE-2023-34454, CVE-2023-34453)
Description	IBM has released a security update addressing Multiple Vulnerabilities exist in in their products. Successful exploitation of these vulnerabilities could lead to denial of service and information disclosure. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	InfoSphere Information Server 11.7 IBM Db2 10.5.0.11 IBM Db2 11.1.4.7 IBM Db2 11.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7010573 https://www.ibm.com/support/pages/node/7011483

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.