Advisory Alert

Alert Number: AAA20210610 **Date:** June 10, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Buffer Overflow
HP	**High , Medium**	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Buffer Overflow (CVE-2021-25217)
Description	Redhat has released Security Update which addresses Buffer Overflow in dhcpd.The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network. ISC has not successfully reproduced the error on a 64-bit system. However, on a 32-bit system it is possible to cause dhclient to crash when reading an improper lease, which could cause network connectivity problems for an affected system due to the absence of a running DHCP client process
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.4 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.4 aarch64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:2359

Affected Product	**HP**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-24511,CVE-2020-12358,CVE-2020-12360,CVE-2020-24486,CVE-2020-12357,CVE-2020-8670,CVE-2020-24512,CVE-2020-24509,CVE-2021-26585)
Description	HP has released Security Updates which address multiple vulnerabilities across several of products.Improper initialization in the firmware for some Intel(R) Processors may allow disclosure of information, escalation of privilege, or denial of service. HPE is releasing firmware updates to mitigate these vulnerabilities.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04168en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04167en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04150en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04159en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04158en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04152en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04155en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04164en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04163en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04162en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04157en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04165en_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.