Advisory Alert

Alert Number: AAA20220112 **Date:** January 12, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	**Multiple Vulnerabilities**
HP	**Critical**	**Multiple Vulnerabilities**
Citrix	**High**	Local privilege Escalation vulnerability

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22947, CVE-2021-36976, CVE-2022-0096, CVE-2022-0097, CVE-2022-0098, CVE-2022-0099, CVE-2022-0100, CVE-2022-0101, CVE-2022-0102, CVE-2022-0103, CVE-2022-0104, CVE-2022-0105, CVE-2022-0106, CVE-2022-0107, CVE-2022-0108, CVE-2022-0109, CVE-2022-0110, CVE-2022-0111, CVE-2022-0112, CVE-2022-0113, CVE-2022-0114, CVE-2022-0115, CVE-2022-0116, CVE-2022-0117, CVE-2022-0118, CVE-2022-0120, CVE-2022-21836, CVE-2022-21837, CVE-2022-21838, CVE-2022-21840, CVE-2022-21841, CVE-2022-21842, CVE-2022-21843, CVE-2022-21846, CVE-2022-21848, CVE-2022-21849, CVE-2022-21850, CVE-2022-21851, CVE-2022-21855, CVE-2022-21857, CVE-2022-21876, CVE-2022-21877, CVE-2022-21880, CVE-2022-21882, CVE-2022-21883, CVE-2022-21887, CVE-2022-21889, CVE-2022-21890, CVE-2022-21892, CVE-2022-21893, CVE-2022-21900, CVE-2022-21901, CVE-2022-21904, CVE-2022-21905, CVE-2022-21907, CVE-2022-21912, CVE-2022-21914, CVE-2022-21915, CVE-2022-21917, CVE-2022-21920, CVE-2022-21922, CVE-2022-21928, CVE-2022-21929, CVE-2022-21930, CVE-2022-21931, CVE-2022-21954, CVE-2022-21958, CVE-2022-21959, CVE-2022-21960, CVE-2022-21961, CVE-2022-21962, CVE-2022-21963, CVE-2022-21964, CVE-2022-21969, CVE-2022-21970, CVE-2022-22709)
Description	Microsoft has released Security Updates addressing multiple vulnerabilities that exists with multiple Microsoft products, features and roles. In addition to security changes for the vulnerabilities, updates include defense-in-depth updates to help improve security-related features. It is highly recommended by Microsoft to apply necessary security fixes at earliest to avoid issues.
Affected Products	.NET Framework Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Graphics Component Microsoft Office Microsoft Office Excel Microsoft Office SharePoint Microsoft Office Word Microsoft Teams Microsoft Windows Codecs Library Open Source Software Role: Windows Hyper-V Tablet Windows User Interface Windows Account Control Windows Active Directory Windows AppContracts API Server Windows Application Model Windows BackupKey Remote Protocol Windows Bind Filter Driver Windows Certificates Windows Cleanup Manager Windows Clipboard User Service Windows Cluster Port Driver Windows Common Log File System Driver Windows Connected Devices Platform Service Windows Cryptographic Services Windows Defender Windows Devices Human Interface Windows Diagnostic Hub Windows DirectX Windows DWM Core Library	Windows Event Tracing Windows Geolocation Service Windows HTTP Protocol Stack Windows IKE Extension Windows Installer Windows Kerberos Windows Kernel Windows Libarchive Windows Local Security Authority Windows Local Security Authority Subsystem Service Windows Modern Execution Server Windows Push Notifications Windows RDP Windows Remote Access Connection Manager Windows Remote Desktop Windows Remote Procedure Call Runtime Windows Resilient File System (ReFS) Windows Secure Boot Windows Security Center Windows StateRepository API Windows Storage Windows Storage Spaces Controller Windows System Launcher Windows Task Flow Data Engine Windows Tile Data Repository Windows UEFI Windows UI Immersive Server Windows User Profile Service Windows User-mode Driver Framework Windows Virtual Machine IDE Drive Windows Win32K Windows Workstation Service Remote Protocol
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan

Affected Product	HP
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-10188)
Description	HP has released Security Updates addressing remote: Arbitrary Code Execution and Buffer Overflow vulnerability that exists in their products. HP-UX telnetd has a potential security flaw that allows remote attackers to execute arbitrary code via short writes or urgent data due to a remote buffer overflow involving the netclear and nextitem functions.
Affected Products	HP-UX 11.31 PHNE_42509 - telnetd Patch 11.31
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04206en_us

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Local privilege Escalation vulnerability (CVE-2022-21825)
Description	Citrix has released Security Updates addressing Local user privilege escalation vulnerability that exists in their products. This vulnerability that could allow a local user to elevate their privilege level to root on the computer running Citrix Workspace app for Linux.
Affected Products	Citrix Workspace App
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX338435

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.