Advisory Alert

Alert Number: AAA20250121 **Date:** January 21, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Remote Unauthorized Data Injection Vulnerabilities
Ubuntu	**Medium**	Linux kernel Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Remote Unauthorized Data Injection Vulnerabilities (CVE-2024-52798)
Description	HPE has released security updates addressing remote unauthorized data injection vulnerabilities in their products. **CVE-2024-52798 -** A potential security vulnerability had been identified in HPE Telco Service Orchestrator software. The vulnerability could be remotely exploited to allow unauthorized data injection. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Service Director - Prior to v5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04770en_us&docLocale=en_US

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Linux kernel Vulnerabilities (CVE-2024-49927, CVE-2024-36893, CVE-2024-49856, CVE-2024-47718, CVE-2024-50015, CVE-2024-50045, CVE-2024-49860, CVE-2024-49866, CVE-2024-49955, CVE-2024-47673, CVE-2024-49948, CVE-2024-47710, CVE-2024-38667, CVE-2024-49959, CVE-2024-44931, CVE-2024-50002, CVE-2024-50033, CVE-2024-50189, CVE-2024-41016, CVE-2024-49924, CVE-2024-50062, CVE-2024-46849, CVE-2023-52532, CVE-2024-50007, CVE-2024-47740, CVE-2024-49969, CVE-2024-50019, CVE-2024-50046, CVE-2024-47692, CVE-2024-46855, CVE-2024-50179, CVE-2024-38545, CVE-2024-50038, CVE-2024-49933, CVE-2024-38538, CVE-2024-27072, CVE-2024-50044, CVE-2024-49867, CVE-2024-49852, CVE-2024-49936, CVE-2024-42079, CVE-2024-50093, CVE-2024-50059, CVE-2024-49903, CVE-2024-47672, CVE-2024-47701, CVE-2024-47712, CVE-2024-49962, CVE-2024-50188, CVE-2024-47723, CVE-2024-47695, CVE-2024-49930, CVE-2024-47697, CVE-2023-52904, CVE-2023-52639, CVE-2024-46854, CVE-2024-49944, CVE-2024-47698, CVE-2024-46865, CVE-2024-49881, CVE-2024-42158, CVE-2024-50024, CVE-2024-46852, CVE-2024-49868, CVE-2024-49895, CVE-2024-49997, CVE-2024-44940, CVE-2023-52917, CVE-2024-50013, CVE-2024-50095, CVE-2024-50001, CVE-2024-50186, CVE-2024-50008, CVE-2024-50006, CVE-2024-47720, CVE-2024-49965, CVE-2024-47705, CVE-2024-49894, CVE-2024-50049, CVE-2024-47748, CVE-2024-49957, CVE-2024-49851, CVE-2024-49877, CVE-2024-49982, CVE-2024-47737, CVE-2024-47742, CVE-2024-47684, CVE-2024-49871, CVE-2024-49902, CVE-2024-47706, CVE-2024-26947, CVE-2024-42156, CVE-2024-49858, CVE-2024-49967, CVE-2024-50191, CVE-2024-47739, CVE-2024-50040, CVE-2024-49879, CVE-2024-49958, CVE-2024-46853, CVE-2024-36968, CVE-2024-46858, CVE-2024-47713, CVE-2024-50096, CVE-2024-50041, CVE-2024-49883, CVE-2024-50039, CVE-2024-35904, CVE-2024-47674, CVE-2024-49913, CVE-2024-49907, CVE-2024-49884, CVE-2024-47747, CVE-2024-49983, CVE-2024-46859, CVE-2024-35951, CVE-2024-47693, CVE-2024-50184, CVE-2024-50035, CVE-2024-49890, CVE-2024-39463, CVE-2024-49875, CVE-2024-49935, CVE-2024-49892, CVE-2024-47696, CVE-2024-49995, CVE-2024-50000, CVE-2023-52621, CVE-2024-49985, CVE-2024-49981, CVE-2024-47690, CVE-2024-50181, CVE-2024-49952, CVE-2024-49975, CVE-2024-44942, CVE-2024-49878, CVE-2024-49973, CVE-2024-50003, CVE-2024-47709, CVE-2024-49900, CVE-2024-50180, CVE-2024-46695, CVE-2024-49889, CVE-2024-49896, CVE-2024-49886, CVE-2024-47699, CVE-2024-50031, CVE-2024-47679, CVE-2024-38544, CVE-2024-49938, CVE-2024-49949, CVE-2024-49946, CVE-2024-47757, CVE-2024-47685, CVE-2024-49966, CVE-2024-47756, CVE-2024-47671, CVE-2024-49882, CVE-2024-49977, CVE-2024-49954, CVE-2024-38632, CVE-2024-49863, CVE-2024-49963, CVE-2024-47734, CVE-2024-47670, CVE-2024-47749, CVE-2024-47735)
Description	Ubuntu has released security updates addressing Linux kernel Vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7166-4

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.