



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Security Updates – HP ThinPro

Tracking #:432316457

Date:31-10-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HP has released a critical security update for HP ThinPro, addressing numerous vulnerabilities across various components.

TECHNICAL DETAILS:

HP has released a critical security update for HP ThinPro, version 8.1 SP4, addressing numerous vulnerabilities across various components. This update, released on October 29, 2024, and last updated on October 30, 2024, is crucial for mitigating potential security risks that could lead to escalation of privilege, arbitrary code execution, denial of service, and information disclosure.

The update addresses vulnerabilities in multiple components, including:

- Python
- BusyBox
- Kerberos
- Wget
- GIFLIB
- Ghostscript
- wpa_supplicant and hostapd
- OpenSSH
- Linux kernel
- Various other libraries and software components

Many of these vulnerabilities have high to critical severity ratings, with CVSS scores ranging up to 9.8

Python Vulnerabilities;

Python, a core component of many systems, has numerous critical vulnerabilities addressed in this update. Notable issues include:

- CVE-2020-27619, CVE-2021-29921, CVE-2019-9636, CVE-2019-10160, CVE-2021-3177, and CVE-2022-48565: All with **CVSS scores of 9.8**, these vulnerabilities could allow remote attackers to execute arbitrary code without authentication
- Several high-severity vulnerabilities (CVSS 7.5) that could lead to denial of service or information disclosure.

Linux Kernel Vulnerabilities:

The Linux kernel, the core of the operating system, has multiple high-severity vulnerabilities addressed:

- CVE-2024-0841, CVE-2024-26934, CVE-2024-27018, CVE-2024-26898, CVE-2024-26929, and CVE-2024-23307: All with CVSS scores of 7.8, these vulnerabilities could allow local attackers to escalate privileges or execute arbitrary code
- Numerous medium-severity vulnerabilities that could lead to denial of service or information leakage

Other Critical Components

- Kerberos: CVE-2024-37371 (**CVSS 9.1**) could allow remote attackers to cause denial of service or potentially execute arbitrary code
- Wget: CVE-2024-38428 (**CVSS 9.1**) could allow remote attackers to execute arbitrary code or disclose information
- OpenSSH: CVE-2024-6387 (CVSS 8.1) could potentially allow remote attackers to bypass

- authentication or execute arbitrary code
- Ghostscript: Multiple high-severity vulnerabilities (CVE-2024-29509, CVE-2024-29506) that could lead to arbitrary code execution

The update also addresses vulnerabilities in components such as BusyBox, GIFLIB, GDK-PixBuf, libarchive, and various other libraries and software packages

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update HP ThinPro systems to the latest version at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.hp.com/us-en/document/ish_11505232-11505266-16/hpsbhf03973