HP publishes a series of critical vulnerabilities in the Teradici PCoIP protocol

HP has warned of serious security vulnerabilities in the Teradici PCoIP client and agent for Windows, Linux, and macOS. These vulnerabilities affect 15 million endpoints.

The computer and software maker discovered that Teradici is affected by a recently disclosed OpenSSL certificate parsing bug. This error causes an infinite denial of service assembly and multiple integer overflow vulnerabilities in Expat.

Teradici PCoIP (PC over IP) is a proprietary computing protocol licensed to many virtualization product vendors. HP acquired Teradici in 2021 and has used PCoIP on its products ever since.

According to HP's official website, Teradici PCoIP products are deployed on 15 million endpoints, supporting government agencies, military units, game developers, broadcast corporations, news companies. ie.

In total, HP announced 12 vulnerabilities with 3 of them being extremely critical (9.8), 8 critical, and 1 moderate.

One of the most critical vulnerabilities patched this time is CVE-2022-0778. This is a denial of service vulnerability in OpenSSL that is triggered by parsing a maliciously crafted certificate.

CVE-2022-0778 will result in a loop that causes the software to become unresponsive. Such an attack would cause disruptions because the user could not access the device remotely.

Other critical vulnerabilities include CVE-2022-22822, CVE-2022-22823 and CVE-2022-22824. All of these vulnerabilities are related to integer overflows and invalid conversions in libexpat that could potentially lead to

uncontrollable resource consumption, elevated privileges, and remote code execution.

The other five critical integer overflow vulnerabilities include CVE-2021-45960, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, and CVE-2021-46143.

Products affected by these vulnerabilities include PCoIP client, client SDK, Graphics Agent, and Standard Agent for Windows, Linux, and macOS.

Users are advised to update to version 22.01.3 or later, using OpenSSL 1.1.1n and libexpat 2.4.7.

HP released security updates on April 4 and 5, 2022, so you can rest assured that you have updated Teradici between then and now.