# Advisory Alert

**Alert Number:** AAA20260616 **Date:** June 16, 2026

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Vendor | Severity | Vulnerability |
|---|---|---|
| **HP** | **Critical** | Out-of-bounds Read Vulnerability |
| **Zyxel Networks** | **High** | Buffer Overflow Vulnerability |
| **HP** | **High**, **Medium** | Multiple Vulnerabilities |
| **IBM** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |
| **Cisco** | **Medium** | Path Traversal Vulnerability |

## Description

| | |
|---|---|
| Vendor | **HP** |
| Severity | **Critical** |
| Affected Vulnerability | Out-of-bounds Read Vulnerability (CVE-2024-5535) |
| Description | HP has released a security update addressing a vulnerability that exists in their product.<br>**CVE-2024-5535:** Calling the OpenSSL API function SSL_select_next_proto with an empty client protocols buffer due to a programming error can trigger a buffer overread, potentially causing a crash or leaking up to 255 bytes of private memory to a peer. However, the issue is rated as low severity and unlikely to be exploited because it requires a specific application configuration error, primarily affects the deprecated NPN protocol rather than the widely used ALPN, and is not under an attacker's control.<br>HP advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | HP One Agent Software Bundled with HP Privacy Settings - Versions prior to 1.3.214.7339 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.hp.com/us-en/document/ish_15146555-15146580-16/hpsbhf04060 |

| | |
|---|---|
| Vendor | **Zyxel Networks** |
| Severity | **High** |
| Affected Vulnerability | Buffer Overflow Vulnerability (CVE-2026-7273) |
| Description | Zyxel Networks has released a security update addressing a vulnerability that exists in their products.<br>**CVE-2026-7273:** A stack-based buffer overflow vulnerability in the CGI program of Zyxel GS1900-48HPv2 firmware versions through 2.90(ABTQ.1)C0 could allow a LAN-based, unauthenticated attacker to exploit the flaw and potentially execute OS commands via a crafted HTTP request.<br>Zyxel Networks advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | • GS1900-8 - Version 2.90(AAHH.1)C0 and earlier<br>• GS1900-8HP - Version 2.90(AAHI.1)C0 and earlier<br>• GS1900-10HP - Versions 2.90(AAZI.1)C0 and earlier<br>• GS1900-16 - Versions 2.90(AAHJ.1)C0 and earlier<br>• GS1900-24 - 2.90(AAHL.1)C0 and earlier<br>• GS1900-24E - 2.90(AAHK.1)C0 and earlier<br>• GS1900-24EP - 2.90(ABTO.1)C0 and earlier<br>• GS1900-24HPv2 - 2.90(ABTP.1)C0 and earlier<br>• GS1900-48 - 2.90(AAHN.1)C0 and earlier<br>• GS1900-48HPv2 - 2.90(ABTQ.1)C0 and earlier |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026 |

| | |
|---|---|
| Vendor | **HP** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-5064, CVE-2024-12797) |
| Description | HP has released a security update addressing multiple vulnerabilities that exist in their products.<br>**CVE-2026-5064:** Potential security vulnerabilities have been identified in the HP One Agent for certain HP PC products, which might allow for escalation of privilege and/or denial of service. HP is releasing software updates to mitigate these potential vulnerabilities.<br>**CVE-2024-12797:** TLS/DTLS clients using RFC7250 Raw Public Keys (RPKs) to authenticate a server may fail to abort the handshake when validation fails, even if SSL_VERIFY_PEER is enabled, leaving connections vulnerable to man-in-the-middle attacks. This issue only affects OpenSSL 3.2+ applications that explicitly enable RPKs and rely solely on the handshake to fail automatically, rather than manually checking the verification results using SSL_get_verify_result().<br>HP advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | HP One Agent Software Bundled with HP Privacy Settings - Versions prior to 1.3.214.7339 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.hp.com/us-en/document/ish_15146555-15146580-16/hpsbhf04060 |

| | |
|---|---|
| Vendor | **IBM** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-40977, CVE-2026-40975, CVE-2026-40973, CVE-2026-22746, CVE-2026-22751, CVE-2026-40542, CVE-2026-22741, CVE-2026-22740, CVE-2026-22731, CVE-2026-22733, CVE-2026-22735, CVE-2026-22737, CVE-2025-67030, CVE-2026-34483, CVE-2026-34487, CVE-2026-34500, CVE-2026-5588, CVE-2026-29181, CVE-2026-0636) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products.<br>These vulnerabilities could be exploited by malicious users to compromise the affected systems. |
| Affected Products | MongoDB Enterprise Advanced with IBM Versions:<br>• migrator 1.0.0 - 1.15.9<br>• jdbc-driver 3.0.0 - 3.0.5<br>• mongodb-kubernetes 1.0.0-1.7.9 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/bulletin/ |

| | |
|---|---|
| Vendor | **Cisco** |
| Severity | **Medium** |
| Affected Vulnerability | Path Traversal Vulnerability (CVE-2026-20262) |
| Description | Cisco has released a security update addressing a vulnerability that exists in their product.<br>**CVE-2026-20262:** This Vulnerability could allow an authenticated, remote attacker to create a file or overwrite any file on the filesystem of an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected API endpoint of the affected system. A successful exploit could allow the attacker to create or overwrite any file on the underlying operating system. This file could later be used to elevate to root.<br>Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Cisco Catalyst SD-WAN Manager |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ |

## 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.