# Advisory Alert

**Alert Number:** AAA20260320 **Date:** March 20, 2026

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Oracle** | **Critical** | Unauthenticated Remote Code Execution Vulnerability |
| **Synology** | **Critical** | Buffer Overflow Vulnerability |
| **NetApp** | **Medium** | Integer Overflow / Wraparound Vulnerability |
| **cPanel** | **Medium**, **Low** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Oracle** |
| Severity | **Critical** |
| Affected Vulnerability | Unauthenticated Remote Code Execution Vulnerability (CVE-2026-21992) |
| Description | Oracle has released a security update addressing a vulnerability that exists in their products.<br>**CVE-2026-21992**: This vulnerability allows an unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager and Oracle Web Services Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager and Oracle Web Services Manager<br>Oracle advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Oracle Identity Manager versions 12.2.1.4.0 and 14.1.2.1.0<br>Oracle Web Services Manager versions 12.2.1.4.0 and 14.1.2.1.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.oracle.com/security-alerts/alert-cve-2026-21992.html |

| | |
|---|---|
| Affected Product | **Synology** |
| Severity | **Critical** |
| Affected Vulnerability | Buffer Overflow Vulnerability (CVE-2026-32746) |
| Description | Synology has released a security update addressing a vulnerability in DiskStation Manager (DSM).<br>**CVE-2026-32746**: telnetd in GNU inetutils through 2.7 allows an out-of-bounds write in the LINEMODE SLC (Set Local Characters) suboption handler because add_slc does not check whether the buffer is full.<br>Synology advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | DSM 7.3 versions prior to 7.3.2-86009-3<br>DSM 7.2.2 versions prior to 7.2.2-72806-8<br>DSM 7.2.1 versions prior to 7.2.1-69057-11 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.synology.com/en-global/security/advisory/Synology_SA_26_03 |

| | |
|---|---|
| Affected Product | **NetApp** |
| Severity | **Medium** |
| Affected Vulnerability | Integer Overflow / Wraparound Vulnerability (CVE-2025-38465) |
| Description | NetApp has released a security update addressing a vulnerability that exists in their products.<br>**CVE-2025-38465**: Certain versions of Linux kernel are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS).<br>NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | FAS/AFF Baseboard Management Controller (BMC) - A900/9500<br>SnapCenter Plug-in for VMware vSphere |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://security.netapp.com/advisory/ntap-20260121-0005 |

| | |
|---|---|
| Affected Product | **cPanel** |
| Severity | **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-3805, CVE-2026-3783, CVE-2026-1965, CVE-2026-3784) |
| Description | cPanel has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems.<br>cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | EasyApache 4 25.51<br>• ea-libcurl: security backports from curl 8.19.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/ |

**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.**