مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates -Dell Elastic Cloud Storage (ECS)

Tracking #:432316679

Date:27-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Dell Technologies has released a security update to address multiple vulnerabilities in Elastic Cloud Storage (ECS).

TECHNICAL DETAILS:

Dell Technologies has released a critical security update (DSA-2024-483) to address multiple vulnerabilities in Elastic Cloud Storage (ECS).

Vulnerabilities Overview:
Third-Party Components:

- **Apache HTTP Server** vulnerabilities (CVE-2024-39573, CVE-2024-38477, CVE-2024-38476, CVE-2024-38475, CVE-2024-38474, CVE-2024-38473, CVE-2023-38709): These vulnerabilities include a variety of security risks, such as remote code execution, privilege escalation, and information leakage. Each of these CVEs could potentially allow attackers to compromise the system if left unpatched.
- **Java** vulnerabilities (CVE-2024-21131, CVE-2024-21138, CVE-2024-21140, CVE-2024-21144, CVE-2024-21145, CVE-2024-21147): These Java-related vulnerabilities pose risks such as denial of service, arbitrary code execution, and potential exploitation in environments that rely on Java-based applications.

Proprietary Code Vulnerabilities:

1. **CVE-2024-51540**: This vulnerability is related to an arithmetic overflow in the retention period handling of ECS. An authenticated user with appropriate access could exploit this flaw to bypass retention policies and potentially delete objects. With a **CVSS base score of 8.1** (high severity), this vulnerability poses a serious risk to the integrity of stored data.
2. **CVE-2024-52534**: This authentication bypass vulnerability enables a low-privileged attacker with remote access to potentially steal session credentials. With a **CVSS base score of 5.4**, this vulnerability could lead to unauthorized access and compromise the security of ECS environments.

Affected Versions:

- Elastic Cloud Storage (ECS): Versions prior to 3.8.1.3.

Fixed Versions:

- ECS 3.8.1.3 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions 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://www.dell.com/support/kbdoc/en-us/000256642/dsa-2024-483-security-update-for-dell-ecs-multiple-vulnerabilities