مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in SailPoint IdentityIQ

Tracking #:432316587

Date:04-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability has been disclosed in SailPoint's IdentityIQ identity and access management (IAM) software, which allows unauthorized access to sensitive content stored within the application directory.

TECHNICAL DETAILS:

A critical security vulnerability (CVE-2024-10905) has been disclosed in SailPoint's IdentityIQ identity and access management (IAM) software, which allows unauthorized access to sensitive content stored within the application directory. This flaw has been assigned a CVSS score of 10.0, indicating maximum severity. It affects versions 8.2, 8.3, 8.4, and earlier versions of IdentityIQ. Attackers could exploit this vulnerability to read files that should otherwise be protected. SailPoint has not yet released an official security advisory, and no additional details are currently available.

Vulnerability Details:

- CVE Identifier: CVE-2024-10905
- Severity: Critical (CVSS v3.1 Score: **10.0**)
- Affected Products: SailPoint IdentityIQ
  - IdentityIQ 8.4 and all patch levels prior to 8.4p2
  - IdentityIQ 8.3 and all patch levels prior to 8.3p5
  - IdentityIQ 8.2 and all patch levels prior to 8.2p8
  - All prior versions
- Vulnerability Description: The flaw allows unauthorized HTTP access to static content stored within the IdentityIQ application directory that should be protected. The vulnerability arises due to improper handling of file names that identify virtual resources (CWE-66), which attackers can exploit to access files that should be inaccessible to them.
- Impact: Successful exploitation of this flaw could allow attackers to read sensitive files in the application directory, potentially exposing confidential information and compromising the integrity of the identity and access management system.

Fixed Versions:

- 8.4p2 or later
- 8.3p5 or later
- 8.2p8 or later
- For all prior versions, update to the latest available patches or consider upgrading to the latest version.

RECOMMENDATIONS:

- Users of SailPoint IdentityIQ are strongly urged to upgrade to the patched versions.
- Access Restrictions: Ensure that static content and sensitive resources within the IdentityIQ application directory are not accessible via HTTP, limiting exposure to unauthorized parties.
- Monitoring & Detection: Implement enhanced monitoring on the IdentityIQ server to detect any suspicious or unauthorized access attempts to the application directory. This may help identify potential exploitation of this vulnerability.
- Security Configuration: Review and adjust security configurations within IdentityIQ to minimize the attack surface, especially focusing on access controls and file handling

mechanisms to prevent unauthorized users from accessing critical content.

- Vendor Communication: Stay informed for any official security advisories or updates from SailPoint. Regularly check their support channels for more information or updates regarding the vulnerability.

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://nvd.nist.gov/vuln/detail/CVE-2024-10905