CVE-2024-55898: IBM I PRIVILEGE ESCALATION

Vairav Advisory Report

Date: 2025-02-24

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability identified as CVE-2024-55898 has been discovered in IBM i versions 7.2, 7.3, 7.4, and 7.5. This flaw allows users with the capability to compile or restore a program to gain elevated privileges due to an unqualified library call. Exploitation of this vulnerability could enable malicious actors to execute code with administrative privileges, potentially leading to full system compromise. The vulnerability has been assigned a CVSS score of 8.5, categorizing it as High severity.

VULNERABILITY DETAILS

CVE-2024-55898

- **Description:** The vulnerability arises from an unqualified library call in IBM i. Users with the ability to compile or restore programs can exploit this flaw to execute user-controlled code with administrative privileges. This could lead to unauthorized actions and potential system compromise.
- **Impact:** Successful exploitation allows attackers to run arbitrary code with administrative rights, leading to potential unauthorized data access, modification, or complete system takeover.
- **CVSS Score:** 8.5 (High)

AFFECTED VERSIONS

IBM i versions:

- 7.2
- 7.3
- 7.4
- 7.5

EXPLOIT DETAILS

IBM is used in logistics, shipping and the trucking business. In environments where IBM i is utilized, users with permissions to compile or restore programs can exploit this vulnerability to escalate their privileges. By leveraging the unqualified library call, attackers can execute code with administrative rights, potentially leading to unauthorized system modifications, data breaches, or service disruptions.

RECOMMENDED ACTIONS

Patch & Upgrade:

IBM has released Program Temporary Fixes (PTFs) to address this vulnerability. Administrators are advised to apply the appropriate PTFs for their IBM i version:

- **IBM i 7.5:** Apply PTFs SJ03650 through SJ04260.
- **IBM i 7.4:** Apply PTFs SJ03651 through SJ04259.
- **IBM i 7.3:** Apply PTFs SJ03652 through SJ04258.
- **IBM i 7.2:** Apply PTFs SJ03653 through SJ04264.

ADDITIONAL SECURITY MEASURES

- **Restrict Compilation and Restoration Privileges**: Limit the ability to compile or restore programs to trusted administrators only, reducing the risk of exploitation by unauthorized users.
- **Monitor System Logs**: Regularly review system logs for unusual activities, especially those related to program compilation or restoration, to detect potential exploitation attempts.
- **Implement Principle of Least Privilege**: Ensure users have only the minimum necessary permissions required for their roles, minimizing potential attack vectors.

REFERENCES

- https://app.opencve.io/cve/CVE-2024-55898
- https://www.ibm.com/support/pages/node/7183835

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com