CVE-2025-0159 - IBM FLASHSYSTEM AUTHENTICATION BYPASS VULNERABILITY

Vairav CVE Report

Date: March 04, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

IBM has disclosed a critical authentication bypass vulnerability (CVE-2025-0159) affecting IBM FlashSystem and IBM Storage Virtualize. This vulnerability enables a remote attacker to bypass authentication on the RPCAdapter endpoint by sending a specially crafted HTTP request. Exploiting this flaw could grant unauthorized access to sensitive system components, posing a significant risk to data integrity and security. Organizations using affected versions should take immediate remediation actions.

VULNERABILITY DETAILS

CVE-2025-0159: IBM FlashSystem Authentication Bypass

Description: This vulnerability arises from improper authentication validation in IBM Storage Virtualize, which allows an unauthenticated attacker to bypass authentication mechanisms by sending specifically crafted HTTP requests to the RPCAdapter endpoint.
Impact: Unauthorized access to critical system components, potential data compromise.
CVSS Score: 9.1 (Critical)

AFFECTED VERSIONS

IBM Storage Virtualize versions:

- 8.5.0.0 through 8.5.0.13
- 8.5.1.0
- 8.5.2.0 through 8.5.2.3
- 8.5.3.0 through 8.5.3.1
- 8.5.4.0
- 8.6.0.0 through 8.6.0.5
- 8.6.1.0
- 8.6.2.0 through 8.6.2.1
- 8.6.3.0
- 8.7.1.0
- 8.7.2.0 through 8.7.2.1

EXPLOIT DETAILS

Attackers can exploit this vulnerability remotely without authentication. By crafting specific HTTP requests, an attacker can bypass security mechanisms, gaining unauthorized access to system functions and potentially exposing or modifying critical data. This flaw could be leveraged to escalate privileges or disrupt normal operations.

RECOMMENDED ACTIONS

- IBM strongly recommends upgrading to the latest secure versions as soon as possible.

ADDITIONAL SECURITY MEASURES

- Restrict network access to IBM Storage Virtualize systems from untrusted sources.
- Implement strict access policies to limit exposure to the RPCAdapter endpoint.
- Enable security logging to detect unauthorized access attempts.
- Conduct periodic vulnerability assessments and apply security best practices.

REFERENCES

https://www.cve.org/CVERecord?id=CVE-2025-0159

https://securityonline.info/cve-2025-0159-cvss-9-1-critical-ibm-storage-flaw-allows-authentication-bypass/

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