CVE-2025-66954 – Buffalo LinkStation Username Enumeration via IDOR

Summary

A vulnerability in **Buffalo LinkStation firmware version 1.85-0.01** allows unauthenticated or guest-level users to enumerate valid usernames and their associated privilege roles.

The issue arises due to improper access control in the `/nasapi` endpoint, enabling **Insecure Direct Object Reference (IDOR)** exploitation.

CVE Information

- **CVE ID:** CVE-2025-66954
- **Status:** Reserved (pending publication)
- **Vendor:** Buffalo
- **Product:** LinkStation
- **Affected Version:** 1.85-0.01
- **Component:** `/nasapi` endpoint
- **Vulnerability Type:** IDOR (Insecure Direct Object Reference)
- **Attack Vector:** Remote

CVSS v3.1 Score

Base Score: 6.5 (Medium)
Vector: `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`

Breakdown

- Attack Vector (AV): Network
- Attack Complexity (AC): Low
- Privileges Required (PR): Low (guest access)
- User Interaction (UI): None
- Scope (S): Unchanged
- Confidentiality (C): High
- Integrity (I): None
- Availability (A): None

Impact

This vulnerability allows attackers with **guest-level access** to:

- Enumerate valid usernames
- Retrieve associated privilege roles
- Access additional user metadata

Exposed Information

- Username
- User ID
- Category
- Role
- Description
- Quota
- Groups
- Primary Group

Security Impact

- **Information Disclosure:** Yes
- **Privilege Escalation (indirect):** Possible via reconnaissance

---

Technical Details

The `/nasapi` endpoint fails to properly validate authorization when handling user-related queries.

By modifying a request parameter, a low-privileged or guest user can retrieve information about other users.

Example Endpoint

/nasapi

Root Cause

- Missing authorization checks
- Insecure direct object reference (IDOR)
- User-controlled parameter not validated

Proof of Concept (PoC)

> Redacted to prevent abuse. Available upon responsible request.

Mitigation

According to the vendor:

Buffalo has confirmed the vulnerability but will not release a patch.

Recommended Mitigation

Disable the **guest user account** to prevent unauthorized access.

Vendor Response

Buffalo has acknowledged the issue and stated:

- No patch will be released
- The exposed data is considered non-critical
- Mitigation is sufficient

Timeline

- **Discovered by:** Zaid Shaikh
- **Vendor Notified:** [Dec 17, 2025]
- **Vendor Response:** Confirmed, no fix planned
- **CVE Reserved:** 2025
- **Public Disclosure:** [Apr 1,2026]

Releases

No releases published

Packages

No packages published

Contributors 1

DBmonster19