CVE-2024-50625

Description

An issue was discovered in Digi ConnectPort LTS prior to version 1.4.12. A vulnerability in the file upload handling of the web application allows manipulation of file paths via POST requests. This can lead to arbitrary file uploads within specific directories, potentially enabling privilege escalation when combined with other vulnerabilities.

Affected Product

- **Vendor:** Digi International Inc.
- **Product:** ConnectPort LTS
- **Versions Impacted:** All versions prior to 1.4.12

Impacted Components

- File Upload Feature
- Path Validation Mechanism
- WebFS Folder

Impact

- **Attack Type:** Local
- **Impact 1:** Code Execution
- **Impact 2:** Denial of Service
- **Impact 3:** Information Disclosure

Attack Vector

On a local area network (LAN) where the product resides, this vulnerability can be exploited via manipulation of file upload paths using specially crafted POST requests. Attackers with specific permissions can upload files to unauthorized directories.

Mitigation and Remediation

- **Immediate Mitigation:** Disable the web service as a temporary workaround while updating to the latest firmware.
- **Fixed Version:** 1.4.12

References

- Digi International Security Advisory for ConnectPort LTS

CWE Identifiers

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-73: External Control of File Name or Path

Discoverer

- **Name:** Cole Chapman
- **Contact:** security.research@endrem.com

CVE-2024-50626

Description

An issue was discovered in Digi ConnectPort LTS prior to version 1.4.12. A Directory Traversal vulnerability exists in WebFS. This allows an attacker on the local area network to manipulate URLs to include traversal sequences, potentially leading to unauthorized access to data.

Affected Product

- **Vendor:** Digi International Inc.
- **Product:** ConnectPort LTS
- **Versions Impacted:** All versions prior to 1.4.12

Impacted Components

- WebFS, a file system for parsing and retrieving URLs

Impact

- **Attack Type:** Local
- **Impact 1:** Denial of Service
- **Impact 2:** Escalation of Privileges
- **Impact 3:** Information Disclosure

Attack Vector

On a local area network (LAN) where the product resides, an attacker could manipulate input fields or URLs to include traversal sequences, potentially gaining unauthorized access to system data.

Mitigation and Remediation

- **Immediate Mitigation:** Disable the web service as a temporary workaround while updating to the latest firmware.
- **Fixed Version:** 1.4.12

References

- Digi International Security Advisory for ConnectPort LTS

CWE Identifiers

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Discoverer

- **Name:** Cole Chapman
- **Contact:** security.research@endrem.com

CVE-2024-50627

Description

An issue was discovered in Digi ConnectPort LTS prior to version 1.4.12. A Privilege Escalation vulnerability exists in the file upload feature. It allows an attacker on the local area network (with specific permissions) to upload and execute malicious files, potentially leading to unauthorized system access.

Affected Product

- **Vendor:** Digi International Inc.
- **Product:** ConnectPort LTS
- **Versions Impacted:** All versions prior to 1.4.12

Impacted Components

- WebFS, a file system for parsing and retrieving URLs
- File Upload Management Page

Impact

- **Attack Type:** Local
- **Impact 1:** Code Execution
- **Impact 2:** Escalation of Privileges

Attack Vector

On a local area network (LAN) where the product resides, an attacker can exploit this vulnerability by uploading a malicious file through the file upload feature, which is executed by the server, potentially allowing unauthorized access or session manipulation.

Mitigation and Remediation

- **Immediate Mitigation:** Disable the web service as a temporary workaround while updating to the latest firmware.
- **Fixed Version:** 1.4.12

References

- Digi International Security Advisory for ConnectPort LTS

CWE Identifiers

- CWE-552: Files or Directories Accessible to External Parties
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

---

Discoverer

- **Name:** Cole Chapman
- **Contact:** security.research@endrem.com

CVE-2024-50628

Description

An issue was discovered in the web services of Digi ConnectPort LTS prior to version 1.4.12. It allows an attacker on the local area network to achieve unauthorized manipulation of resources, which may lead to remote code execution when combined with other issues.

Affected Product

- **Vendor:** Digi International Inc.
- **Product:** ConnectPort LTS
- **Versions Impacted:** All versions prior to 1.4.12

Impacted Components

- WebFS, a file system for parsing and retrieving URLs

Impact

- **Attack Type:** Local
- **Impact 1:** Code Execution

Attack Vector

On a local area network (LAN) where the product resides, the vulnerability can be exploited remotely by sending specially crafted HTTP requests, potentially allowing unauthorized actions on the server.

Mitigation and Remediation

- **Immediate Mitigation:** Disable the web service as a temporary workaround while updating to the latest firmware.
- **Fixed Version:** 1.4.12

References

- Digi International Security Advisory for ConnectPort LTS

CWE Identifiers

- CWE-749: Exposed Dangerous Method or Function
- CWE-20: Improper Input Validation

Discoverer

- **Name:** Cole Chapman
- **Contact:** security.research@endrem.com