SECURITY ADVISORY

INFINITT-SA-2026-001

INFINITT ULite Security Update — Share-Link and Web Interface Vulnerabilities

PUBLISHED	LAST UPDATED	STATUS
November 5, 2026	November 5, 2026	Fix available

SUMMARY

INFINITT Healthcare has released a security update for INFINITT ULite that addresses vulnerabilities in the web share-link functionality and the web interface. The issues were identified through a coordinated vulnerability disclosure by an external security research firm. INFINITT has released fixed builds and is deploying the update to affected customers under existing maintenance agreements.

There is no indication that these vulnerabilities have been exploited.

AFFECTED PRODUCTS

PRODUCT	AFFECTED VERSIONS	FIXED VERSION
INFINITT ULite	`5.0.2.1_BN48_20260528` and earlier 5.0.2.1 builds	`5.0.2.1 BN50`

VULNERABILITY INFORMATION

The update addresses the following issues:

Reflected cross-site scripting (XSS) in the web interface

A crafted link could cause unintended script to run in the context of a user's session in the affected page.

Share-link access control weakness

Weaknesses in the generation and protection of share links could allow unauthorized access to shared content.

CVE identifiers assigned to these issues will be listed in the References section once published. Detailed technical information is intentionally withheld to protect customers until the update has been broadly deployed.

REMEDIATION

Customers should ensure their INFINITT ULite installation is updated to build `BN50` or later.

INFINITT is coordinating and performing this update directly with affected customer sites under existing maintenance agreements. No customer action is required beyond scheduling the update with INFINITT; customers who have questions about their patch status should contact their INFINITT support representative.

ACKNOWLEDGEMENTS

INFINITT Healthcare thanks **SecureMind Sàrl** for responsibly reporting these issues and for coordinating their disclosure.

REFERENCES

- `CVE-2026-19876`
- `CVE-2026-19877`

CONTACT

For questions regarding this advisory, please contact INFINITT Healthcare Product Security at cybersecurity@infinitt.com.