مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in CrushFTP

Tracking #:432317079

Date:15-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities in CrushFTP. These vulnerabilities could allow malicious actors to perform Server-Side Request Forgery (SSRF) and Directory Traversal attacks, potentially leading to information disclosure and other security risks.

TECHNICAL DETAILS:

Vulnerabilities Details:

CVE-2025-32102: Server-Side Request Forgery (SSRF)

- A Server-Side Request Forgery (SSRF) vulnerability exists in the /WebInterface/function/ URI. By manipulating the host and port parameters within a command=telnetSocket request, an attacker can potentially force the CrushFTP server to make requests to arbitrary internal or external hosts and ports. This can be exploited to perform port scanning of internal networks or interact with internal services.
- Successful exploitation of this vulnerability could allow an attacker to gather information about internal network infrastructure and potentially access internal services.

CVE-2025-32103: Directory Traversal

- A Directory Traversal vulnerability exists in the /WebInterface/function/ URI. The application does not adequately sanitize the path parameter in a command=getAdminXMLListing request. This allows an attacker to inject Universal Naming Convention (UNC) paths (e.g., \\\\server\\share) instead of local file paths. As a result, the CrushFTP server can be tricked into listing directories and files accessible via SMB on remote network shares, bypassing intended security restrictions.
- Successful exploitation of this vulnerability could allow an attacker to view the directory structure and potentially access sensitive files located on accessible network shares. This bypasses the SecurityManager restrictions that are in place for local file system access.

Affected Versions:

- CrushFTP 9.x versions
- CrushFTP 10.x versions up to and including 10.8.4
- CrushFTP 11.x versions up to and including 11.3.1

Mitigation:

- Update CrushFTP to the latest version

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by CrushFTP.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://seclists.org/fulldisclosure/2025/Apr/17