مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Zero-Day Vulnerability in CrushFTP

Tracking #:432317514

Date:22-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical zero-day vulnerability in CrushFTP. This vulnerability allows remote, unauthenticated attackers to exploit the HTTP(S) interface, resulting in unauthorized administrative access and potentially complete compromise of affected systems.

TECHNICAL DETAILS:

A critical zero-day vulnerability (**CVE-2025-54309**) (CVSS 9.0) has been identified in CrushFTP, a secure file transfer server widely used in enterprise environments. This vulnerability allows remote, unauthenticated attackers to exploit the HTTP(S) interface, resulting in unauthorized administrative access and potentially complete compromise of affected systems. The flaw is actively exploited in the wild.

Impact

- **Remote Code Execution** with administrative privileges
- **Creation of unauthorized admin-level accounts**
- **Malware deployment** and other server manipulations
- Disruption of business-critical file transfer operations

Indicators of Compromise (IOCs)

- Unauthorized changes to:
  CrushFTP/users/MainUsers/default/user.XML
- Presence of last_logins field in user.XML (this is **not** normal)
- Creation of suspicious **long random user IDs** with administrative rights
  e.g., 7a0d26089ac528941bf8cb998d97f408m
- Any unknown accounts with administrative privileges

Affected Versions:

- CrushFTP Version 10: All builds below 10.8.5
- CrushFTP Version 11: All builds below 11.3.4_23

Fixed Versions:

- CrushFTP Version 10: 10.8.5 or later
- CrushFTP Version 11: 11.3.4_23 or later

RECOMMENDATIONS:

If compromise is suspected, administrators should:

1. **Restore the default user profile** from backups **prior to July 16, 2025**:
   - Navigate to: CrushFTP/users/MainUsers/default
   - Replace or delete user.XML to trigger auto-recreation of a clean default user.
2. **Use non-native archive tools** (e.g., **WinRAR**, **WinZip**, **macOS Archive Utility**) when extracting backups to ensure proper file restoration.
3. **Review logs** for suspicious upload/download activity.
4. **Immediately upgrade to the latest secure build**:
   - Version 10: **10.8.5 or later**
   - Version 11: **11.3.4_23 or later**

To prevent similar incidents and improve overall security posture:

- **Restrict administrative access** to trusted IP addresses
- **Enable automatic updates** to stay current with patches
- **Whitelist** only necessary and verified IP ranges
- **Deploy a DMZ instance** in enterprise environments for added protection

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://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025