مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in CrushFTP

Tracking #:432316663

Date:24-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in CrushFTP, a popular file transfer server. This security flaw could potentially result in account takeovers.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-53552**
- CVSS Score: 9.8 (Critical)
- The vulnerability stems from CrushFTP's mishandling of password reset requests. Attackers can manipulate the password reset email link, and if a user clicks on this malicious link, their account can be compromised, giving the attacker full control.

Affected Versions:

- CrushFTP 10 (versions before 10.8.3)
- CrushFTP 11 (versions before 11.2.3)

Fixed Versions:

- CrushFTP version 10.8.3, 11.2.3, or later

RECOMMENDATIONS:

- **Update Immediately**: upgrade the affected versions to the fixed versions at the earliest.
- **Configure Email Reset URLs**: Restrict password reset emails to trusted domains.
- **Monitor Server Logs**: Regularly check for any suspicious activity.
- **User Education**: Train users to be cautious of unexpected password reset emails and avoid clicking on suspicious links.
- **Enable MFA**: Where possible, implement multi-factor authentication
- **Review User Accounts**: Audit for any unauthorized new user accounts or recent password changes

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=Update