مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

CrushFTP Zero-Day Vulnerability

Tracking #:432315775

Date:22-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed CrushFTP, a popular file transfer software, has a critical zero-day vulnerability actively exploited in targeted attacks.

TECHNICAL DETAILS:

CrushFTP has identified a critical zero-day vulnerability that is actively being exploited by threat actors. This vulnerability poses a significant risk to systems running CrushFTP, potentially leading to unauthorized access and data compromise. Immediate action is required to mitigate this threat and safeguard sensitive information.

Vulnerability: CrushFTP Virtual File System Escape (CVE-TBD)
Impact: Unauthenticated attackers can potentially download sensitive system files.
Exploitation: Actively exploited in targeted attacks, possibly for intelligence gathering.
Affected Versions: CrushFTP versions below v11

Fixed Versions:

- CrushFTP v11.1.0

RECOMMENDATIONS:

- Apply the latest CrushFTP update (v11 or later) as soon as possible.
- Isolate CrushFTP servers within a Demilitarized Zone (DMZ) to limit access from the public internet.
- Increase monitoring for suspicious activity on CrushFTP servers.

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