Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

A Zero-Day Vulnerability in CrushFTP Results in Server Compromise

Date of Publication	Admiralty Code	TA Number
April 25, 2024	A1	TA2024164

Summary

Discovered On: 19 April 2024
Affected Products: CrushFTP
Impact: The discovery of an actively exploited zero-day vulnerability, CVE-2024-4040, in CrushFTP is concerning. This vulnerability allows unauthenticated attackers to bypass the user's virtual file system (VFS) and access system files for download.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-4040	CrushFTP VFS Sandbox Escape Vulnerability	CrushFTP	✓	✓	✓

Vulnerability Details

#1 The recent discovery of CVE-2024-4040, a zero-day vulnerability in CrushFTP, highlights a critical security risk. This vulnerability allows unauthenticated attackers to evade the user's virtual file system (VFS) and access system files, posing a significant threat to server security. CrushFTP, designed for secure file transfer between clients and servers, offers robust monitoring of server activities across networks, making the prompt application of patches essential to maintain system security..

#2 The CrushFTP vulnerability poses a severe risk as it allows remote attackers to exploit server-side template injection techniques. By leveraging this vulnerability, attackers can bypass authentication mechanisms, granting them unauthorized access to the CrushFTP server. This could potentially compromise the entire CrushFTP instance, endangering the security and integrity of stored data. Attackers may exploit this vulnerability to read files from the filesystem outside of the Virtual File System (VFS) Sandbox and execute remote code on the affected server.

#3 This vulnerability has been actively exploited in wild. The vulnerability affected all CrushFTP versions below 10.7.1 and 11.1.0, including legacy versions. It is especially important to note that this vulnerability was particularly targeted at organizations in the United States.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4040	CrushFTP versions prior to 10.7.1 and 11.1.0	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*	CWE-1336

Recommendations

Update: Kindly update your CrushFTP servers to the latest version 10.7.1 or 11.1.0, which fixes the issues of the CVE-2024-4040 vulnerability.

Endpoint Protection: Deploy reputable endpoint protection software that includes anti-malware and behavior-based detection capabilities to identify and block suspicious activities on endpoints.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation	

Patch Details

Administrators should promptly update the CrushFTP servers to version 10.7.1 or 11.1.0 to ensure that they are protected against the vulnerability.

Link: https://www.crushftp.com/download.html

References

https://www.rapid7.com/blog/post/2024/04/23/etr-unauthenticated-crushftp-zero-day-enables-complete-server-compromise/

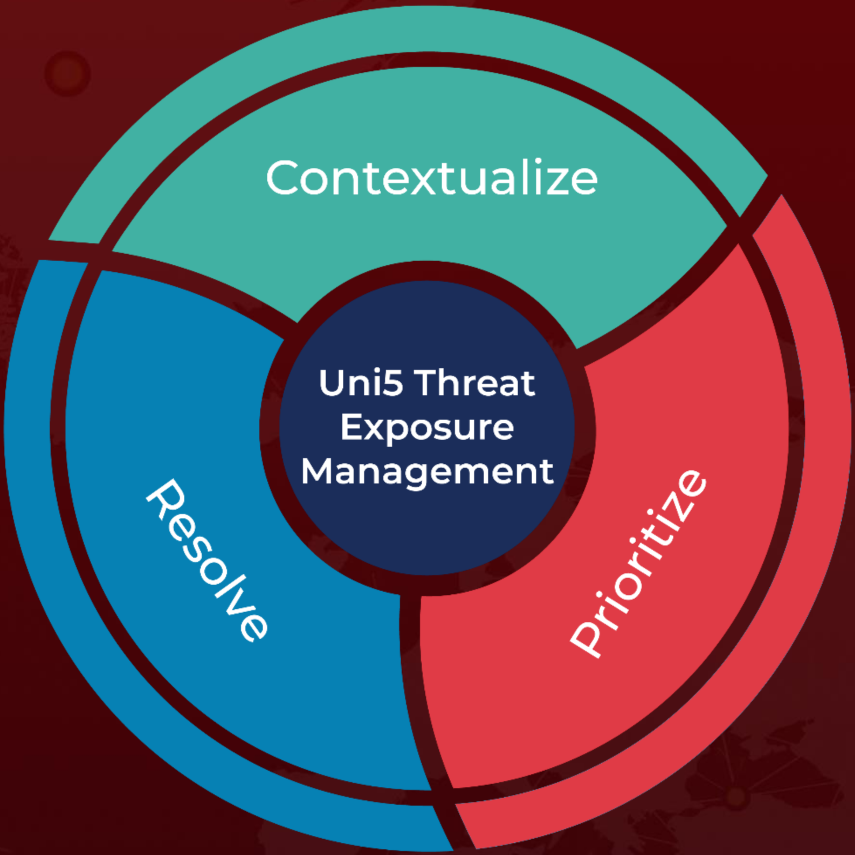
https://twitter.com/Shadowserver/status/1783399676521168935

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 25, 2024 • 7:10 AM

More at www.hivepro.com