Fortinet VPN Zero-Day Exploited in Active Malware Attacks

Overview

A zero-day vulnerability in Fortinet's FortiClient VPN client for Windows is being actively exploited by an APT through its DEEPDATA malware framework. DeepData is a surveillance framework utilizing various plugins to extract sensitive data from browsers, communication apps, and password managers, while also supporting audio recording through the system's microphone.

This unpatched vulnerability allows attackers to extract VPN credentials directly from the memory of compromised systems. It is a credential disclosure vulnerability in FortiClient for Windows and has been unpatched since July 2024. Credentials, including usernames, passwords, and server information, remain in memory post-authentication, allowing for exploitation. Affected products include Fortinet FortiClient VPN Client for Windows (latest version analyzed - v7.4.0).

According to an analysis by the security firm Volexity, the DeepData framework is attributed to the APT BrazenBamboo (APT41), a state-sponsored threat group associated with China. This group is also linked to the development of the LightSpy malware and the DeepPost tool, which is designed for post-exploitation data exfiltration.

BrazenBamboo leverages compromised VPN accounts to establish initial access to corporate networks, which allows them to move laterally and infiltrate systems. While there isn't a patch for the credential disclosure vulnerability, there are recommendations that organizations can apply until Fortinet issues a patch. Please see the recommendations below.

Aspire Protects

- **Patch –** When a patch is available, Aspire's CTI team will update this notice. Apply Fortinet-provided mitigation steps when they become available.
- For detailed technical analysis, see Volexity's report on DEEPDATA and related vulnerabilities.
- Disable FortiClient VPN usage on critical systems until a patch is available.
- Restrict access to VPN services through multi-factor authentication (MFA).
- Enforce least-privilege access to mitigate exploitation impact.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190): Exploiting FortiClient zero-day vulnerability to establish initial access.

Credential Access

- Credential Dumping (T1003): Extracting stored VPN credentials from process memory.

Exfiltration

- Exfiltration Over C2 Channel (T1041): Using HTTPS and WebSocket for secure data exfiltration.

IoCs

IPv4

- 103[.]255[.]176[.]176
- 103[.]27[.]109[.]217
- 103[.]27[.]109[.]28
- 103[.]43[.]17[.]99
- 103[.]43[.]18[.]22
- 202[.]43[.]239[.]13
- 45[.]125[.]34[.]126
- 103[.]27[.]108[.]122
- 103[.]43[.]18[.]95
- 118[.]195[.]234[.]243
- 119[.]147[.]213[.]48
- 154[.]91[.]196[.]185
- 203[.]83[.]10[.]112
- 203[.]83[.]9[.]60
- 203[.]83[.]9[.]62
- 207[.]148[.]77[.]93
- 222[.]219[.]183[.]84
- 38[.]55[.]97[.]178
- 43[.]248[.]136[.]104
- 43[.]248[.]136[.]110
- 43[.]248[.]136[.]215

- 45[.]155[.]220[.]194
- 45[.]155[.]220[.]79

MD5

- 4b9aa7d571be1a6ec62931c4c6624328
- 6ce2477efe7e853cea90764db5a64e6e
- 7efb1bc15ee6e3043f8eaefcf3f10864
- fb99f5da9c0c46c27e17dc2dc1e162d7

SHA1

- 4b2aed91ab914d22e2fd45a644fa121143c9c8e0
- 5ac2ef263f328980062217135f2d0c359811dbd4
- 7e3547211fa4d314b40b6812730d100cd43edc2c
- a77204b049f622b6995c223d0f5f53118cc72f37

SHA256

- 041c13a29d3bee8d2e4bd9d8bde8152b5ac8305c1efcc198244b224e33635282
- 213520170fc7113ac8f5e689f154f5c8074dd972584b56d820c19d84b7e5b477
- 2bfb82a43bb77127965a4011a87de845242b1fb98fd09085885be219e0499073
- 2cede95138f60dfaee4aa3538962ca2ab7dada376dd3977d56e0e6e208001a73
- 37a1ffaba2e3ea9a7b2aa272b0587826cc0b5909497d3744ec8c114b504d2544
- 460f1a00002e1c713a7753293b4737e65d27d0b65667b109d66afca873c23894
- 4fd541e0c899260511c5c0ebd5ccaa134078d50d268a35af60e22422673c48ee
- 55e2dbb906697dd1aff87ccf275efd06ee5e43bb21ea7865aef59513a858cf9f
- 666a4c569d435d0e6bf9fa4d337d1bf014952b42cc6d20e797db6c9df92dd724
- 724351b5cc9ad496a6c9486b8ef34772f640590a90293f913f005e994717134b
- 735d59c0949e258501e177ec2dd5fbb60df9fa401ace08949b89077c6f0d41d0
- 88e5ca44189dabb4cec8a183f6268a42f3f92b2c6d7c722d7f55efd3dc5334c8
- a560931baa404189257ec9cbcc2b9449c579018218cc1d70c99b1d36dd292a0e
- ac7e20d4ddccc5e249ff0c1a72e394f9c1667a896995cf55b97b4f9fbf5de2fd
- b523cdd1669dbd7ab68b43fd20f30a790ec0351876a0610958b9405468753a10
- b79629e820cdd36d0daed964a2c0338e125a1f90f08e226f52dc60070747c62e
- c0d4517e0727e94887d3b8a2c6c69938930995a8bcf37c9dafbd3a86b042417c
- c3995f28476f7a775f4c1e8be47c64a300e0f16535dc5ed665ba796f05f19f73
- ccfd6ef35c718e2484b3727035d162b667f4b56df43324782d106f50ed1e3bcc
- cf59cd171270ec9bc2baf618838eb57802cc9d48f64205da308406811dd4da92
- efff4106cfd21a356b13a5a99c626a4f103f03b9491c0f1f5e135c1e3c84e76c
- f0fc2c418e012e034a170964c0d68fee2c0efe424a90b0f4c4cd5e13d1e36824

URLs

- hxxp://103.255.176[.]176:28992/
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/Audio[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/ChatIndexedDb[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/OutlookX32[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/ProductList[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/SocialSoft[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/Tdm[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/WebBrowser[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/data[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/frame[.]dll
- hxxp://119.147.213.48:28992/asdgdsfdsfasd/localupload[.]exe
- hxxp://202.43.239.13:28992/asdgdsfdsfasd/ChatIndexedDb[.]dll
- hxxp://202.43.239.13:28992/asdgdsfdsfasd/SocialSoft[.]dll
- hxxp://202.43.239.13:28992/asdgdsfdsfasd/SystemInfo[.]dll
- hxxp://202.43.239.13:28992/asdgdsfdsfasd/appdata[.]dll

Targeted Industries

- The targeted industries for this vulnerability includes:
    - Government and Defense - Espionage on critical national security information.

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
    - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately

maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

BrazenBamboo Weaponizes FortiClient Vulnerability to Steal VPN Credentials via DEEPDATA | Volexity