

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

DEEPDATA Empowers the Exploitation of Fortinet Flaw

Date of Publication

November 21, 2024

Last Update Date

March 19, 2025

Admiralty Code

A1

TA Number

TA2024439

Summary

Attack Commenced: July 2024

Threat Actor: BrazenBamboo

Malware: DEEPDATA, LIGHTSPY

Affected Product: FortiClient

Attack Region: Worldwide

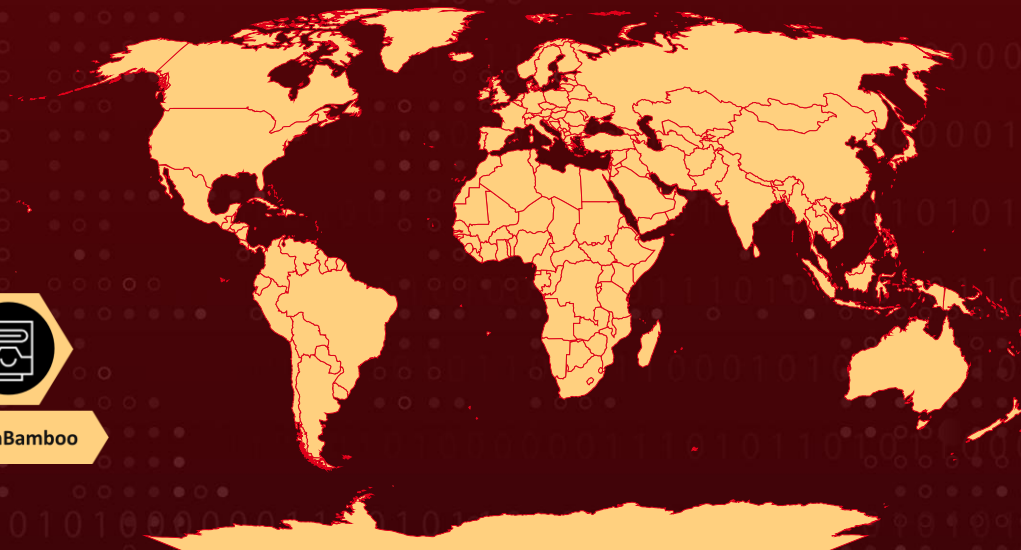
Attack: Chinese threat actors, known as BrazenBamboo, are actively exploiting a zero-day vulnerability in Fortinet's FortiClient Windows VPN client with the DEEPDATA post-exploitation toolkit. This critical flaw enables attackers to extract user credentials from memory after VPN authentication, echoing a similar vulnerability reported in 2016.



Attack Regions



BrazenBamboo



CVE

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin
Powered by Bing

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH LINK
CVE-2024-50570	Fortinet Cleartext Storage of Sensitive Information Vulnerability	FortiClientWindows , FortiClientLinux			



Attack Details

#1

Chinese threat actors identified as BrazenBamboo have been observed exploiting a zero-day vulnerability in Fortinet's FortiClient Windows VPN client through a custom post-exploitation toolkit known as DEEPDATA. This vulnerability allows attackers to extract user credentials from memory after successful VPN authentication. Notably, this flaw mirrors a 2016 issue in FortiClient, where hardcoded memory offsets similarly exposed credentials.

#2

The DEEPDATA toolkit is a modular post-exploitation framework designed to gather sensitive information from compromised Windows systems. Operating via command-line execution, its FortiClient plugin utilizes a library file, msenvico.dll, to exploit the zero-day vulnerability. Once deployed, the plugin retrieves VPN credentials directly from the process memory of the FortiClient application.

#3

In addition to the FortiClient plugin, DEEPDATA includes multiple plugins supporting a broad range of espionage-related functionalities, such as extracting files, system information, and credentials. The toolkit also integrates with DEEPPOST, a data exfiltration tool used to transfer stolen data to attacker-controlled systems.

#4

By exploiting FortiClient accounts, BrazenBamboo can gain initial access to corporate networks, enabling lateral movement, access to sensitive systems, and the expansion of their espionage campaigns. The LIGHTSPY malware family, previously linked to the Chinese-affiliated group APT41, has similarly demonstrated cross-platform adaptability.

#5

LIGHTSPY variants now target macOS, iOS, and most recently, Windows. This evolving threat highlights the critical risks associated with vulnerabilities in widely deployed software, as sophisticated threat actors continue to enhance their toolkits for broader, more impactful operations.

Recommendations



Utilize SAML Authentication: Users leveraging SAML authentication through FortiClient's built-in browser remain secure as long as the FortiClient console is configured to close automatically after establishing a VPN connection. Organizations should ensure this setting is enabled to prevent security loopholes.



Enable Two-Factor Authentication: To minimize the risk of stolen passwords, it is recommended to enable two-factor authentication (2FA) for all user accounts in FortiOS. This adds an additional layer of security beyond passwords.



Ensure FortiClient Console Auto-Closes (Windows 7.2.6 & 7.4.1): For FortiClient Windows versions 7.2.6 and 7.4.1, it is essential to verify that the console window automatically closes after a VPN connection is established. This is the default setting, but administrators should confirm that it remains enabled. This configuration can also be managed centrally using EMS (Endpoint Management Server) by enabling the "Minimize FortiClient Console on Connect" option in the EMS Remote Access Profile. To enforce this, the XML configuration file should include the following line:

```
<minimize_window_on_connect>1</minimize_window_on_connect>
```



Monitor and Analyze Network Activity: Turn on detailed logging for VPN access and monitor logs regularly for unusual activity or unauthorized access attempts. Utilize IDS solutions to detect suspicious activities or potential breaches related to the VPN.



Implement Zero Trust Architecture: Adopt a Zero Trust security model that requires verification for every user and device attempting to access the network resources, minimizing unauthorized access risks.



Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0005</u> Defense Evasion	<u>TA0006</u> Credential Access
<u>TA0007</u> Discovery	<u>TA0009</u> Collection	<u>TA0011</u> Command and Control	<u>TA0010</u> Exfiltration
<u>TA0042</u> Resource Development	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.003</u> Windows Command Shell	<u>T1071</u> Application Layer Protocol
<u>T1071.001</u> Web Protocols	<u>T1083</u> File and Directory Discovery	<u>T1584</u> Compromise Infrastructure	<u>T1587</u> Develop Capabilities



<u>T1587.001</u> Malware	<u>T1587.004</u> Exploits	<u>T1133</u> External Remote Services	<u>T1078</u> Valid Accounts
<u>T1543</u> Create or Modify System Process	<u>T1562</u> Impair Defenses	<u>T1212</u> Exploitation for Credential Access	<u>T1005</u> Data from Local System

Indicators of Compromise (IOCs)

TYPE	VALUE
File Names	deepdata.zip, data.dll, mod.dat, readme.txt, frame.dll, ffmpeg.dll, vertdll.dll, iumdll.dll, ucrtbase_enclave.dll, d3dcompiler_47.dll, config.json, manifest.json, manifest1.json, date.ini
MD5	b9129d83af902908fa7757e906ec0afe, 0f0fadd0546734c5c82f3c33d8268046, 7efb1bc15ee6e3043f8eaefcf3f10864, d66776ee123ef2947bc3175653a68d05, ea47fd87c1b109d5fd529c213aea6b30, 8625c0cf0748d04d43db54884ee13672, 4b9aa7d571be1a6ec62931c4c6624328, 7529f56dde7a8302947982c43080bfcc, 6ce2477efe7e853cea90764db5a64e6e, fb99f5da9c0c46c27e17dc2dc1e162d7, 48f8b7e0db439336549b93bda8633cd2, d521bf0f24c839e7ceb5db77de090fbc, 3b61d82be05f18754238e26b835da103, 847ec30a4ff2391f1eb7669c22940e51, bdd8926f4be6576653ac96ee732d587a, e79da1e448c60e12d835b47735f9da03, 533297a7084039bf6bda702b752e6b82

TYPE	VALUE
SHA1	20214e2e93b1bb37108aa1b8666f6406fabca8a0
File Paths	D:\Code\OtherWork\DeepDataH\bin\data.pdb, D:\tmpWork\deepdata-v2\deepdata\bin\frame.pdb, G:\xmh_miqu_key\xmh\密取\appdata\Release\appdata.pdb, G:\xmh_miqu_key\xmh\密取\appdata\Release\Whatsapp.pdb, G:\xmh_miqu_key\xmh\密取\appdata\Release\signal.pdb, G:\xmh_miqu_key\xmh\密取\SystemInfo\Release\SystemInfo.pdb, E:\zyx\dll\Dll1\Debug\wifiList.pdb, D:\tmpWork\deepdata-v2\deepdata\bin\x86\WebBrowser.pdb, G:\xmh_miqu_key\xmh\密取\Pass\Release\Pass.pdb, G:\xmh_miqu_key\xmh\密 \outlook\outlook_2022.12.14\OUTLOOK\Bin\OutlookX32.pdb, E:\zyx\dll\ProductList\Debug\ProductList.pdb, D:\tmpWork\deepdata-v2\deepdata\bin\x86\SocialSoft.pdb, C:\Users\GT1\source\repos\Audio_miqu\Release\Audio.pdb, C:\Users\GT1\source\repos\Audio_miqu\Release\audio.core.pdb, G:\xmh_miqu_key\xmh\密取 \ChatIndexedDb\Release\ChatIndexedDb.pdb, E:\xmh\密取\appdata\Release\Whatsapp.pdb, D:\Code\project\MiQuH\MiQuH\Release\Tdm.pdb, D:\CodeS\compile\tg471\tdesktop\out\Release\Telegram.pdb
SHA256	666a4c569d435d0e6bf9fa4d337d1bf014952b42cc6d20e797db6c9df 92dd724, cf59cd171270ec9bc2baf618838eb57802cc9d48f64205da308406811 dd4da92, ac7e20d4ddccc5e249ff0c1a72e394f9c1667a896995cf55b97b4f9fbf5 de2fd, ccfd6ef35c718e2484b3727035d162b667f4b56df43324782d106f50e d1e3bcc, 37a1ffaba2e3ea9a7b2aa272b0587826cc0b5909497d3744ec8c114b 504d2544, 213520170fc7113ac8f5e689f154f5c8074dd972584b56d820c19d84b 7e5b477, 460f1a00002e1c713a7753293b4737e65d27d0b65667b109d66afca8 73c23894, b523cdd1669dbd7ab68b43fd20f30a790ec0351876a0610958b94054 68753a10, 041c13a29d3bee8d2e4bd9d8bde8152b5ac8305c1efcc198244b224e 33635282, 2bfb82a43bb77127965a4011a87de845242b1fb98fd09085885be219 e0499073, 724351b5cc9ad496a6c9486b8ef34772f640590a90293f913f005e994 717134b,

TYPE	VALUE
SHA256	55e2dbb906697dd1aff87ccf275efd06ee5e43bb21ea7865aef59513a 858cf9f, b79629e820cdd36d0aed964a2c0338e125a1f90f08e226f52dc6007 0747c62e, 88e5ca44189dabb4cec8a183f6268a42f3f92b2c6d7c722d7f55efd3dc 5334c8, 735d59c0949e258501e177ec2dd5fbb60df9fa401ace08949b89077c 6f0d41d0, efff4106cfd21a356b13a5a99c626a4f103f03b9491c0f1f5e135c1e3c8 4e76c, a560931baa404189257ec9cbcc2b9449c579018218cc1d70c99b1d36 dd292a0e, c0d4517e0727e94887d3b8a2c6c69938930995a8bcf37c9dafbd3a86 b042417c, f0fc2c418e012e034a170964c0d68fee2c0efe424a90b0f4c4cd5e13d1 e36824, 2cede95138f60dfaee4aa3538962ca2ab7dada376dd3977d56e0e6e2 08001a73, 4fd541e0c899260511c5c0ebd5ccaa134078d50d268a35af60e22422 673c48ee, c3995f28476f7a775f4c1e8be47c64a300e0f16535dc5ed665ba796f0 5f19f73, 035db9a3bc9bfba542583c9350baa39741018127a27e7e3ebb6e9f50 ddb96f41, 0b8c9d991162efca3c34d3d97b79f8edfd45ec3e052c4fef080523bacd 586d11, 0c4ebc3d96911af9878343ee8dcba7f79a64cf86ae9b8e6cdc7bbb100 177b9af, 151edcd7d877048d5e8fce9919477cbe5c2de4bd65cd46aa228528dd 00360db1, 1bfb7c520335f96c1b268bd9e59688fca49e67e5785aa2a5a3bb2814 84318101, 37c74a4a8bbe272da16f956eea69f0dcbf0caeb0d3da72d084502499c 124b879, 3d9f8e1e84e9cfc742bc51742863a325eda1ea459ed6a6a5b2c47710f c171848, 424aaacf3444fe51b9865af3079777a977111cab9a329494f1f12c0a4 8dbffa7, 51b83c5732fbfc8da9d333e7daea85725c04f241f27648708d326077a 4556717, 5d39dd90ee6e01afbe070030d863385adf5976752274f95f936c1b62 41f78d6a, 7008e312446919cceb73db951af89602aaa9312c0c793b9bbb2e1a30 6f84d82f, 72bfd0f5299809c66a1fea743d5bd6559d031052bc31ced95884aeb8 60f318a1,



TYPE	VALUE
SHA256	742fd59971ac576e579a45d8f2d4165c4c18b08685880fd457be1651523b5da4, 75dadf4ead9e1b3ad73fb135a5950534d0a9e58bdb4c6f2dbd4ca8b7f66b4a56, 765ef96d1f46aca2c2b816f92e57b92ba8126a601e76a9377d742eb6bb2d95ef, 83c610c4a56aa15a2220d2c3b05e0ff073f6ffb97f892118ae10c03b1bee35b0, 84edc435eac5543a01c5aa1391e73e5dfe49f6b6fd577750204d514f1caaa9b4, 87daf1ee49925271f0f3b2f5671ef028d9e6b79d487a68b879103a752d6fdb7f, 87f9766eb91e966a7599f65d16a696fea6452383d298be65635e63dfac226976, 91b3e5e9ea4b1d7dc188dec0b28afa53f1048b4162ec9dbd60a458b650410585, af0de88e8b17d628b354b5586da7718b06755d88ddde8c933c8606018e5ed7ff, b208b73d003a8ee0eb24ce09f7ff515e18229d1836c43159a8e1821615aab19c, c782346bf9e5c08a0c43a85d4991f26b0b3c99c054fa83beb4a9e406906f011e, d4aea0bbfe5b309f2464fef8ebb44dd514f8162d41be53b423c64b4acb4a5ee6, dab112f7c765a375f0f12313d1b1e3cf14963113cf7b6f101ba5192a0c3874de, dbf0ee5e96b418bb6237772262701baf213bf60ede3ed7d90c126117097aa3ec, ee7c3e2352a4e7bf37e3d76972de1ba493c0be26832cae5978c134155ac7835b, fc1c30f6f23a303944d8d04c6c0a7f21b137f70f60ce4f03b2e930f3e98a91da, 0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c, 08e0ed3c9a4c04a4cb83e17f14a4959236dda048336c04e30ab7786b5bf8ffa7, 80c0cdb1db961c76de7e4efb6aced8a52cd0e34178660ef34c128be5f0d587df, 0f662991dbd0568fc073b592f46e60b081eedf0c18313f2c3789e8e3f7cb8144, 3d6ef4d88d3d132b1e479cf211c9f8422997bfcaa72e55e9cc5d985fd2939e6d, 18bad57109ac9be968280ea27ae3112858e8bc18c3aec02565f4c199a7295f3a, 5fb67d42575151dd2a04d7dda7bd9331651c270d0f4426acd422b26a711156b5,



TYPE	VALUE
SHA256	65aa91d8ae68e64607652cad89dab3273cf5cd3551c2c1fda2a7b90aed2b3883, 4511567b33915a4c8972ef16e5d7de89de5c6dffe18231528a1d93bfc9acc59f, d2ccbf41552299b24f186f905c846fb20b9f76ed94773677703f75189b838f63, 2b4fbd5aa06f70d84091d2f7cca4bd582237f1a1084835c3c031a718b6e283f9, ac6d34f09fcac49c203e860da00bbbe97290d5466295ab0650265be242d692a6, fc7e77a56772d5ff644da143718ee7dbaf7a1da37cceb446580cd5efb96a9835, be02ce6964d1a10b48897466846e0889c7cf54bdf34133f52bc9226feb31548, e5f0022cd79fad21c760a57fedff48e559aaf80ac0e8bbf44401b465654aba02, 4cbc692e0c914e235b92c55e910c818ec014461462736c56e5328dbc b9971756, fd261e970d01f0f123e32baf02f5f32edd0db1ee3ffc6c44d18565ecf1194630, 7d4c9e9b73f74426a975a5f8584059e8c8ca24418e7994ec83ef735c84cf2d31, ea2c0cbd35465dad118d69fdbf37ecfb9b0eca461e9854d2790dd98201af6dc4, 205e62b04478c0ef69d69970716e5cb9e5d03293157733194d95ea801df3726c, d804e5cde29c10fa3ca56386c147706d9501b6c2fb73f8fd329a24b9acb4c4e0
Network Indicators	119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/WebBrowser[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/localupload[.]exe, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/Tdm[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/OutlookX32[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/SocialSoft[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/ChatIndexedDb[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/Audio[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/ProductList[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/frame[.]dll, 119[.]147[.]213[.]48[:]:28992/asdgdsfdfsasd/data[.]dll, 202[.]43[.]239[.]13[:]:28992/asdgdsfdfsasd/SystemInfo[.]dll, 202[.]43[.]239[.]13[:]:28992/asdgdsfdfsasd/ChatIndexedDb[.]dll, 202[.]43[.]239[.]13[:]:28992/asdgdsfdfsasd/SocialSoft[.]dll, 202[.]43[.]239[.]13[:]:28992/asdgdsfdfsasd/appdata[.]dll, 103[.]255[.]176[.]176[:]:28992/ asdgdsfdfsasd/Telegram[.]dll

TYPE	VALUE
IPv4	45[.]155[.]220[.]79, 45[.]155[.]220[.]194, 45[.]125[.]34[.]126, 43[.]248[.]136[.]215, 43[.]248[.]136[.]110, 43[.]248[.]136[.]104, 38[.]55[.]97[.]178, 222[.]219[.]183[.]84, 203[.]83[.]9[.]62, 203[.]83[.]9[.]60, 203[.]83[.]10[.]112, 202[.]43[.]239[.]13, 154[.]91[.]196[.]185, 119[.]147[.]213[.]48, 118[.]195[.]234[.]243, 103[.]43[.]18[.]95, 103[.]43[.]18[.]22, 103[.]43[.]17[.]99, 103[.]27[.]109[.]28, 103[.]27[.]109[.]217, 103[.]27[.]108[.]122, 207[.]148[.]77[.]93, 43[.]248[.]136[.]241, 103[.]43[.]19[.]64, 121[.]201[.]109[.]98, 103[.]27[.]110[.]159, 49[.]232[.]185[.]137, 103[.]43[.]19[.]245, 58[.]221[.]58[.]240, 47[.]236[.]30[.]141, 27[.]124[.]37[.]30, 27[.]124[.]37[.]59, 27[.]124[.]37[.]64, 103[.]27[.]108[.]207, 103[.]27[.]108[.]205, 47[.]238[.]155[.]170, 124[.]156[.]48[.]83, 103[.]27[.]108[.]152, 47[.]238[.]153[.]120

Patch Details

A security patch has been released to address vulnerabilities in FortiClient across multiple platforms, including Linux, Mac, and Windows. Users are advised to upgrade to the latest recommended versions to mitigate potential risks. Specifically, FortiClientLinux users should upgrade to version 7.4.3, 7.2.8, or 7.0.14 or above. FortiClientMac users should upgrade to 7.4.3, 7.2.8, or migrate to a fixed release for version 7.0. FortiClientWindows users should upgrade to 7.4.2, 7.2.7, or 7.0.14 or above. These updates contain important security fixes that enhance system protection against potential threats. Immediate action is recommended to maintain system security and integrity.

Link:

<https://fortiguard.fortinet.com/psirt/FG-IR-23-278>

References

<https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/>

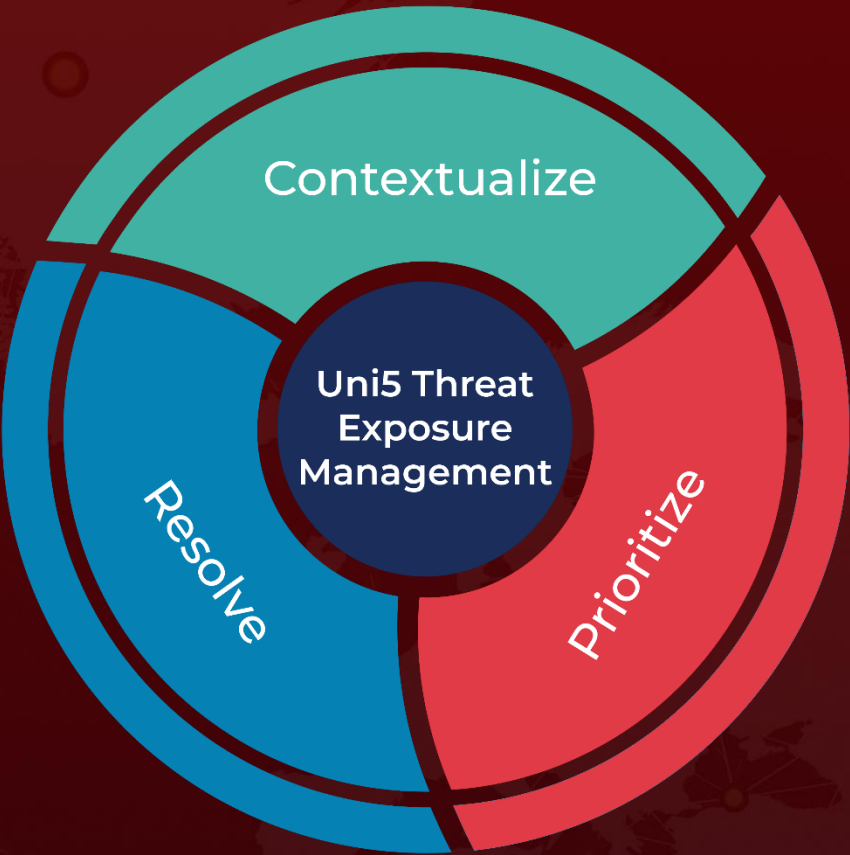
<https://blogs.blackberry.com/en/2024/11/lightspy-apt41-deploys-advanced-deepdata-framework-in-targeted-southern-asia-espionage-campaign>

<https://www.threatfabric.com/blogs/lightspy-implant-for-ios>

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
November 21, 2024 • 5:00 AM

