

February 21, 2024

# A Catastrophe For Control: Understanding the ScreenConnect Authentication Bypass (CVE-2024-1709 & CVE-2024-1708)

By:  Team Huntress

On February 19, 2024, ConnectWise published a [security advisory](#) for ScreenConnect version 23.9.8, referencing two vulnerabilities and software weaknesses. The same day, Huntress researchers worked to understand this threat and successfully recreated a proof-of-concept exploit demonstrating its impact.

This write-up will discuss our analysis efforts and the technical details behind this attack, which we’re coining as “SlashAndGrab.”

The ConnectWise advisory indicated that in all versions of ScreenConnect below 23.9.8 there were two vulnerabilities:

- CVE-2024-1709:** Authentication bypass using an alternate path or channel (CWE-288)
- CVE-2024-1708:** Improper limitation of a pathname to a restricted directory (“path traversal”) (CWE-22)

The first vulnerability was disclosed with a critical base CVSS scoring of 10, the highest possible severity. The authentication bypass would ultimately open the door for the second vulnerability.

ConnectWise made a patch available and expressed that all **on-premise** versions of ScreenConnect 23.9.7 and below must be updated immediately—cloud instances were already automatically patched.

At the time of release, the ConnectWise advisory was very sparse on technical details. There was not much information available as to what these vulnerabilities really consisted of, how they might be taken advantage of, or any other threat intelligence or indicators of compromise to hunt for.

Once we recreated the exploit and attack chain, we came to the same conclusion: there should not be public details about the vulnerability until there had been adequate time for the industry to patch. It would be too dangerous for this information to be available.

## Categories

### Response to Incidents

## See Huntress in action

Our platform combines a suite of powerful managed detection and response tools for endpoints and Microsoft 365 identities, science-backed security awareness training, and the expertise of our 24/7 Security Operations Center (SOC).

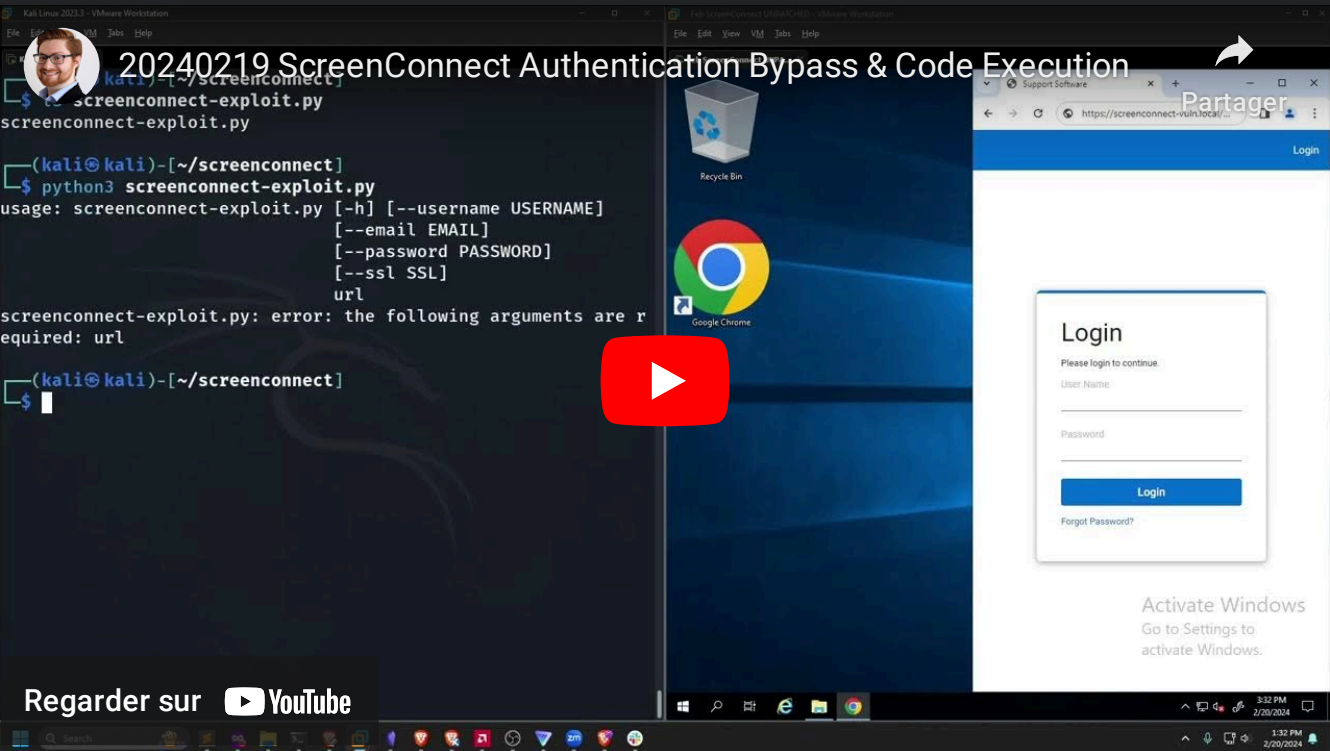
Book a Demo

Share



The “exploit” is trivial and embarrassingly easy.

Below is a video demonstration of our recreated proof-of-concept exploit, which performs the simple authentication bypass but takes it a step further to showcase remote code execution.



## Our Analysis

When the Huntress team was made aware of the ConnectWise advisory, our team began to dig into what changes were made in the patch that could help explain what these vulnerabilities were.

We could simply look for the differences between code present in the new, patched version, and the previous, unpatched version. Creating a local testing environment for both of these states of the ScreenConnect software, we could easily see the delta that might clue us into the potential exploit.

We observed that these files differed:

1	ScreenConnect/App_Data/User.xml
2	ScreenConnect/Bin/ScreenConnect.WindowsFileManager.exe
3	ScreenConnect/Bin/ScreenConnect.ClientService.exe
4	ScreenConnect/Bin/ScreenConnect.Client.Agent.zip
5	ScreenConnect/Bin/ServedArtifacts/ScreenConnect.Windows.dll
6	ScreenConnect/Bin/ServedArtifacts/ScreenConnect.Core.dll
7	ScreenConnect/Bin/ScreenConnect.Core.jar
8	ScreenConnect/Bin/ScreenConnect.Service.exe
9	ScreenConnect/Bin/ScreenConnect.WindowsClient.exe
10	ScreenConnect/Bin/ScreenConnect.WindowsServer.dll
11	ScreenConnect/Bin/ScreenConnect.Server.dll
12	ScreenConnect/Bin/ScreenConnect.ClientSetup.exe
13	ScreenConnect/Bin/ScreenConnect.Client.exe.jar
14	ScreenConnect/Bin/ScreenConnect.Web.dll
15	ScreenConnect/Bin/ScreenConnect.Client.Bundle.zip
16	ScreenConnect/Bin/ScreenConnect.Windows.dll
17	ScreenConnect/Bin/ScreenConnect.ClientSetup.msi
18	ScreenConnect/Bin/ScreenConnect.WindowsInstaller.dll
19	ScreenConnect/Bin/ScreenConnect.WindowsBackstageShell.exe
20	ScreenConnect/Bin/ScreenConnect.Client.apk
21	ScreenConnect/Bin/ScreenConnect.Client.dll
22	ScreenConnect/Bin/ScreenConnect.Client.application
23	ScreenConnect/Bin/ScreenConnect.Client.exe
24	ScreenConnect/Bin/ScreenConnect.Core.dll
25	ScreenConnect/Bin/ScreenConnect.Relay.dll

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

# CVE-2024-1709 – Authentication Bypass

Most of these changes observed in the new version were binary files, which require decompilation to compare; however, `SetupWizard.aspx` is a text file. When looking at the differences in this file, it immediately looked promising:

```
11a2
2> <%@ Implements Interface="ScreenConnect.ISetupHandler" %>
35a7,14
4>
5>     protected override void OnInit(EventArgs e)
6>     {
7>         base.OnInit(e);
8>
9>         if (SetupModule.IsSetup)
1>             throw new InvalidOperationException("Already setup");
1>     }
```

SetupWizard.aspx.diff hosted with ❤️ by GitHub

view raw

In the newest update, we can see there is a new check to ensure that the instance is set up before allowing the user to use the setup wizard. This piqued our interest as, at face value, version 23.9.7 already blocked access to the setup wizard after authentication. Looking closer into `ScreenConnect.SetupModule` inside of `ScreenConnect.Web.dll` sheds more light on the exploitation path.

In previous versions of ScreenConnect, this handler was registered for the `OnBeginRequest` event, while in 28.9.8 it is registered for the `OnPostMapRequestHandler` event. This was seemingly done so that the `context.Handler` field will be populated. A new check is added to validate if the resolved HTTP handler implements the new `ISetupHandler` interface whereas the old code simply checked that `Request.Path` string matched `"/SetupWizard.aspx"`. This change implies that there was some way to bypass the string comparison of `Request.Path` in previous versions. **If the request path does not match `"/SetupWizard.aspx,"` then the setup wizard will be allowed regardless of the setup state of the instance.**

This would normally not be exploitable, but .Net has weird functionality that allows URL path components after a mapped legitimate URL to be passed along to the application. This information is exposed in `Request.FilePath`, `Request.PathInfo` and `Request.Path`. For example, if there is a legitimate path `"/something.aspx"`, then .Net will allow the user to request `"/something.aspx/anythingelse"` and will pass along the trailing bit after the file path via the `Request.PathInfo`. However, `Request.Path` always contains *both* `Request.FilePath` *and* `Request.PathInfo` per [MSDN documentation](#):

Putting this together, it means we can simply request `"/SetupWizard.aspx/literallyanything"` and we should be allowed to access the

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

immediately after clicking the “Next” button on the setup page, so there is no need to complete the setup wizard fully to exploit the system (i.e. you do not need to replace or have access to a valid license key). **Completing this step will completely overwrite the internal user database. All other local users will be deleted aside from the user you specify in the setup wizard.**

Once you have administrative access to a compromised instance, it is trivial to create and upload a malicious ScreenConnect extension to gain Remote Code Execution (RCE). This is not a vulnerability, but a feature of ScreenConnect, which allows an administrator to create extensions that execute .Net code as **SYSTEM** on the ScreenConnect server.

## CVE-2024-1708 – Path Traversal

The second vulnerability referenced in the ConnectWise ScreenConnect advisory presents a risk of ZipSlip attacks. We observed changes to **ScreenConnect.Core.dll**:

```
111057c11057
2<      public void ExtractAllEntries(string basePath)
3---
4>      public void ExtractAllEntries(string basePath, string
511062c11062
6<      FileSystemExtensions.DemandInParentPath
7---
8>      FileSystemExtensions.DemandInParentPath

ScreenConnect.Core.dll.cs.diff hosted with ❤ by GitHub view raw
```

and **ScreenConnect.Server.dll**:

```
18392a8393
2>      DirectoryInfo extensionsDirectory = GetExtensionsDirectory
38398c8399
4<      zipFile.ExtractAllEntries(GetExtensionsDirectory
5---
6>      zipFile.ExtractAllEntries(extensionsDirectory)

ScreenConnect.Server.dll.cs.diff hosted with ❤ by GitHub view raw
```

This adds new function arguments to strictly handle file paths when extracting content from a ZIP file. Looking through the code base, we can see these utility functions only seem to be used when handling ScreenConnect extensions. Prior to this patch, a malicious extension could potentially write files anywhere within **C:\Program Files (x86)\ScreenConnect\App\_Extensions** instead of being properly restricted to their extension subdirectory.

While this is another vulnerability fixed in version **23.9.8** that could lead to remote code execution in certain conditions, it relies upon having administrative credentials and access to be able to use the Extensions functionality. This capability is “unlocked” by the authentication bypass, but is less severe on its own.

In our recreated proof-of-concept exploit, taking advantage of this potential ZipSlip attack vector was not necessary; after gaining administrator access with the authentication bypass, it was already possible to run arbitrary code with the typical Extensions feature set. The primary difference being that malicious code written using this vulnerability does not necessarily need an installed extension to execute. This means that it may go unnoticed more easily within your environment. Any **.aspx** or **.ashx** files within

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

While researching the above vulnerabilities, Huntress identified Indicators Of Compromise (IOCs) and developed a set of detections that can be used to notify ScreenConnect users of potential malicious activity.

As a reminder, per Huntress’s previous [post](#), the below listed SIGMA rules that leverage [Windows Event ID 4663](#) requires that the Advanced Auditing policy be configured, and an appropriate SACL applied to the directory. Please refer to the previous blog post for how to generate this event.

## CVE-2024-1709 – Authentication Bypass

While replicating the Authentication Bypass exploit, Huntress observed IIS logs for the malicious **SetupWizard.aspx** URL path, which can be used as an indicator of compromise:

The following Sigma rule will detect requests made to **SetupWizard.aspx** with a trailing path segment. This behavior is never legitimate, and should clearly indicate malicious intent if observed in the wild.

```
1title: CVE-2024-1709 - ScreenConnect Authentication Bypass Exploitation
2id: d27eabad-9068-401a-b0d6-9eac744d6e67
3status: experimental
4description: |
5    Detects GET requests to '/SetupWizard.aspx/[anythinghere]' that :
6references:
7    - https://www.connectwise.com/company/trust/security-bulletins/con
8    - https://www.huntress.com/blog/a-catastrophe-for-control-understa
9    - https://www.cve.org/CVERecord?id=CVE-2024-1709
10author: Matt Anderson, Huntress
11date: 2024/02/20
12tags:
13    - attack.initial_access
14    - attack.persistence
15    - cve.2024.1709
16logsource:
17    category: webserver
18detection:
19    selection:
20        cs-uri-stem|contains: '/SetupWizard.aspx/'
21    condition: selection
22falsepositives:
23    - Unknown
24level: critical
```

SetupWizard\_sigma\_rule.yml hosted with ❤️ by GitHub [view raw](#)

After accessing the Setup Wizard, an attacker will input new credentials to gain access to Screen Connect. Doing so will write a new user database to a temporary XML file. The following Sigma rule can be used to detect the ScreenConnect server writing to a temporary XML file on the server. While this may be an indicator of compromise, this activity is known to also be observed when legitimately modifying local users or their permissions in ScreenConnect, so there is a non-zero false positive rate.

```
1title: ScreenConnect User Database Modification
2id: 4109cb6a-a4af-438a-9f0c-056abba41c6f
```

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline



```
9author: Huntress DE&TH Team
10date: 2024/02/20
11logsource:
12  product: windows
13  service: security
14  definition: 'Requirements: SACLs must be enabled for the ScreenConnect
15detection:
16  selection:
17    EventID: 4663
18    ObjectType: 'File'
19    AccessMask: '0x6'
20    ObjectName|endswith: '.xml'
21    ObjectName|contains|all:
22      - 'Temp'
23      - 'ScreenConnect'
24    ProcessName|contains: ScreenConnect.Service.exe
25  condition: selection
26falsepositives:
27  - Unknown
28level: medium
29tags:
30  - cve.2024.1709
```

ScreenConnect\_modification\_sigma\_rule.yml hosted with ❤ by GitHub

view raw

The following YARA rule is similar to the IIS log Sigma rule given above. It will detect IIS log entries that reference **SetupWizard.aspx** with a trailing path component. As mentioned previously, a trailing path component on this file is always associated with malicious activity.

```
1rule ScreenConnect_CVE_2024_1709_Exploitation {
2  meta:
3    description = "Detects a GET request to '/SetupWizard.aspx/' with
4    author = "Huntress DE&TH Team"
5    reference = "https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass"
6    date = "2024-02-20"
7    id = "2886530b-e164-4c4b-b01e-950e3c40acb4"
8  strings:
9    $s1 = "/SetupWizard.aspx/" ascii
10
11  condition:
12    $s1
13}
```

SetupWizard\_IIS\_log.yara hosted with ❤ by GitHub

view raw

## CVE-2024-1708 – Path Traversal

The path traversal exploit allows attackers to write files within the root of the **App\_Extensions** directory. The following Sigma rule should alert on file modifications at the root of the **App\_Extensions** directory while excluding legitimate modifications to extensions themselves.

```
1title: CVE-2024-1708 - ScreenConnect Path Traversal Exploitation
2id: 4c198a60-7d05-4daf-8bf7-4136fb6f5c62
3status: experimental
4description: This detects file modifications to ASPX and ASHX files within
5references:
6  - https://www.connectwise.com/company/trust/security-bulletins/connectwise-cve-2024-1708
7  - https://www.cve.org/CVERecord?id=CVE-2024-1708
8  - https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass
author: Huntress DE&TH Team
```

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

```
16 product: windows
17 service: security
18 definition: 'Requirements: SACLs must be enabled for the ScreenConnect
19detection:
20 selection:
21     EventID: 4663
22     ObjectType: 'File'
23     ProcessName|contains: 'ScreenConnect.Service.exe'
24     AccessMask: '0x6'
25     ObjectName|endswith:
26         - 'ScreenConnect\\App_Extensions\\*.ashx'
27         - 'ScreenConnect\\App_Extensions\\*.aspx'
28 legitimate_path:
29     ObjectName|contains: 'ScreenConnect\\App_Extensions\\*\\'
30 condition: selection and not legitimate_path
31falsepositives:
32 - Unknown
33level: critical
```

App\_Extensions\_sigma\_rule.yml hosted with ❤ by GitHub [view raw](#)

We encourage customers and partners to reach out if they need assistance. If you are not currently using Huntress and need help monitoring for activity related to this vulnerability, you can [use Huntress' free trial](#).

## You Might Also Like

Incident Response: A Choose Your Own Adventure Exercise

[Learn More](#)

Cracks in the Foundation: Intrusions of FOUNDATION Accounting Software

[Learn More](#)

SlashAndGrab: The ConnectWise ScreenConnect Vulnerability Explained

[Learn More](#)

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

Platform

Huntress Managed Security Platform

Managed EDR

Managed EDR for macOS

MDR for Microsoft 365

Managed SIEM

Managed Security Awareness Training

Book A Demo

Solutions

Phishing

Compliance

Solutions by Topic

Business Email Compromise

Healthcare

Manufacturing

Education

Finance

Why Huntress?

Managed Service Providers

Value Added Resellers

Business & IT Teams

24/7 SOC

Case Studies

Resources

Resource Center

Blog

Upcoming Events

Support Documentation

About

Our Company

Leadership

News & Press

Careers

Contact Us

Free Trial

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline