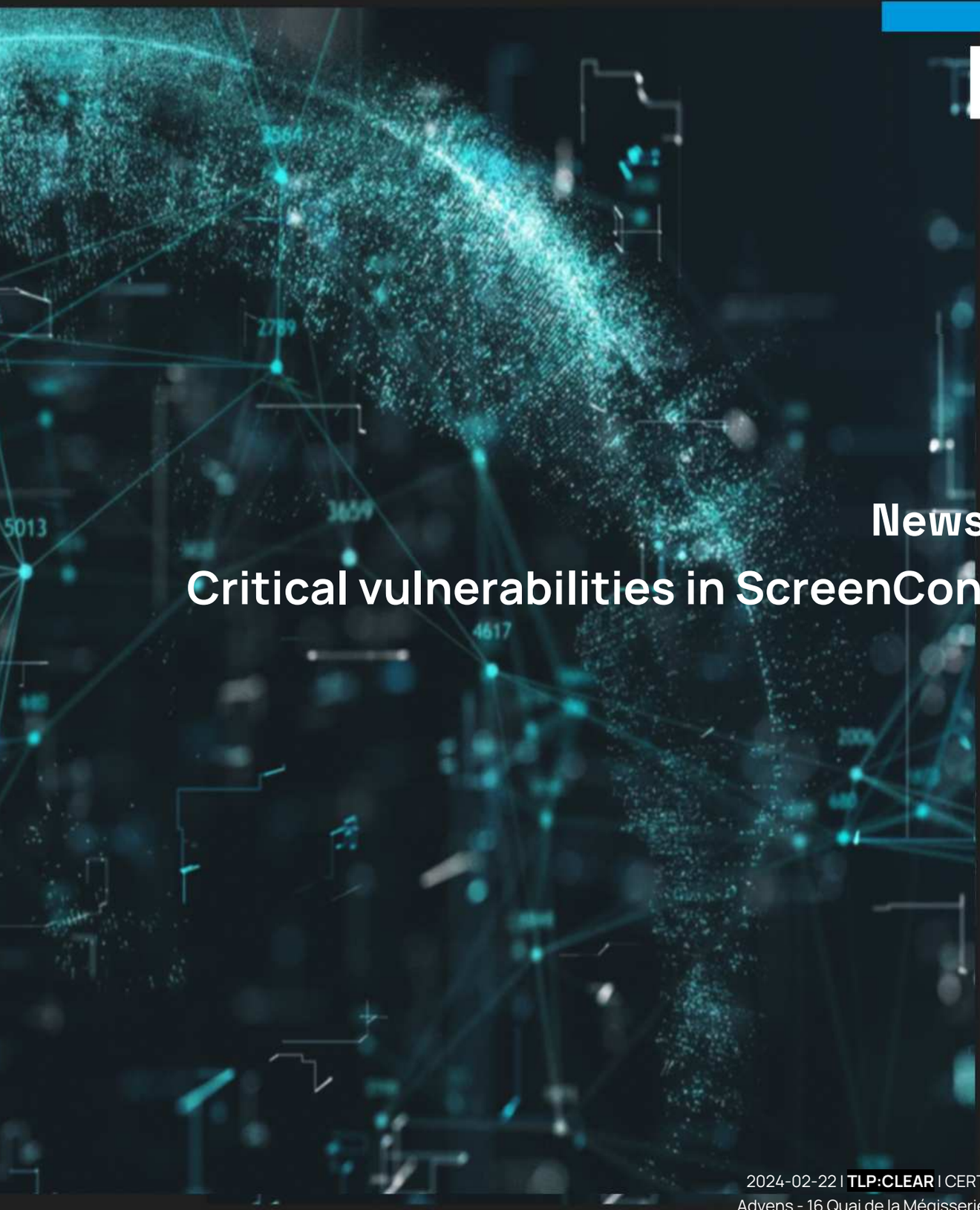
aDvens

Security for the greater good



Newscast

Critical vulnerabilities in ScreenConnect

2024-02-22 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

Table of content

ConnectWise ScreenConnect

On 19 February 2024, ConnectWise published a security advisory for their remote access tool ScreenConnect. This bulletin follows the disclosure of two vulnerabilities on 13 February 2024 through their vulnerability disclosure platform Connectwise Trust Center. No CVE IDs have been assigned yet.

Update from 22 February 2024: CISA assigned CVE-2024-1708 and CVE-2024-1709 identifiers to these two vulnerabilities affecting *ConnectWise ScreenConnect*. ConnectWise also changed the update recommendations in its advisory on 21 February 2024 and removed license restrictions for products that are no longer under maintenance.

CVE-2024-1709

Due to an access control flaw, an unauthenticated attacker can access ScreenConnect's setup wizard, normally restricted to authenticated users. This vulnerability allows them to create an administrator account and gain access to confidential data. The exploit is trivial.

This vulnerability is exploited.

Type of vulnerability

- CWE-288: Authentication bypass using an alternate path or channel

Risks

- Authentication bypass
- Data confidentiality breach

Severity (Base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- ConnectWise ScreenConnect 23.9.7 and prior

Recommendations

- Update ConnectWise ScreenConnect to version 23.9.8 for on-premise and self-hosted installations.
- Additional information is available in ConnectWise's advisory.

Update from 22 February 2024: ConnectWise released version 23.9.10.8817 with fixes to improve customer experience in addition to patch vulnerabilities. In this latest version, license restrictions were removed to upgrade products that are no longer under maintenance.

Proof of concept

A proof of concept is availabe in open source.

Detection

- The exploit involves a change to the **C:\Program Files (x86)\ScreenConnect\AppData\User.xml** file. This file contains all created users and last login dates. A new user with a recent connection could indicate a compromise.
- Configuration of an Advanced auditing policy to log 4663 events and a system access control list (SACL) set on directory **C:\Windows\Temp\ScreenConnect\<ScreenConnectVersion>** can detect a modification to the previous file.

Sigma

```
title: ConnectWise ScreenConnect SetupWizard Authentication Bypass (Feb 2024)
id: d27eabad-9068-401a-b0d6-9eac744d6e67
status: experimental
description: Detects http requests to '/SetupWizard.aspx/' that indicate exploitation of the ScreenConnect
vulnerability.
references:
  - https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
  - https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8
  - https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
author: Huntress DE&TH Team
date: 2024/02/20
logsource:
  category: webserver
  product: windows
detection:
    selection:
      cs-uri-query|contains: '/SetupWizard.aspx/'
    condition: selection
falsepositives:
    - Unknown
level: critical
tags:
  - attack.initial_access
  - attack.persistence
```

```
title: ConnectWise ScreenConnect SetupWizard User Database Modification
id: 4109cb6a-a4af-438a-9f0c-056abba41c6f
status: experimental
description: This detects file modifications to the temporary xml user database file indicating local user
modification in the ScreenConnect server. This will occur during exploitation of the ScreenConnect
Authentication Bypass vulnerability in versions <23.9.8, but may also be observed when making legitimate
modifications to local users or permissions. This requires an Advanced Auditing policy to log a successful
Windows Event ID 4663 events and with a SACL set on the directory.
references:
    - https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
    - https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8
    - https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
author: Huntress DE&TH Team
date: 2024/02/20
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4663
        ObjectType: 'File'
        ProcessName|contains:
            - 'ScreenConnect.Service.exe'
        AccessMask: 0x6
        ObjectName|endswith: '.xml'
        ObjectName|contains|all:
            - 'Temp'
            - 'ScreenConnect'
    condition: selection
falsepositives:
    - Unknown
level: critical
tags:
  - attack.initial_access
  - attack.persistence
```

Yara

```
rule ConnectWise_ScreenConnect_Authentication_Bypass_Feb_2024_Exploitation_IIS_Logs {
   meta:
      description = "Detects an http request to '/SetupWizard.aspx/' with anything following it, which when
found in IIS logs is a potential indicator of compromise of the 2024 ConnectWise ScreenConnect (versions
prior to 23.9.8) vulnerability that allows an Authentication Bypass"
      author = "Huntress DE&TH Team"
      reference = "https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-
23.9.8"
      date = "2024-02-20"
      id = "2886530b-e164-4c4b-b01e-950e3c40acb4"
   strings:
      $s1 = "/SetupWizard.aspx/" ascii
   condition:
      $s1
}
```

CVE-2024-1708

This Path Traversal vulnerability allows an attacker with high privileges to carry out a Zip Slip attack and remotely execute arbitrary code. Privilege escalation can be achieved with the exploit of the first vulnerability.

Type of vulnerability

- **CWE-22** : Improper limitation of a pathname to a restricted directory (“path traversal”)

Risk

- Remote code execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	High	Impact on integrity	High
User Interaction	Required	Impact on availability	High

Impacted Products

- ConnectWise ScreenConnect 23.9.7 and prior

Recommendations

- Update ConnectWise ScreenConnect to version 23.9.8 for on-premise and self-hosted installations.
- Additional information is available in ConnectWise's advisory.

Update from 22 February 2024: ConnectWise released version 23.9.10.8817 with fixes to improve customer experience in addition to patch vulnerabilities. In this latest version, license restrictions were removed to upgrade products that are no longer under maintenance.

Proof of concept

A proof of concept is availabe in open source.

Detection

- Configuration of an Advanced auditing policy to log 4663 events and a system access control list (SACL) set on directory ***C:\Program Files (x86)\ScreenConnect\App_Extensions** can detect the writing of **.aspx** or **.ashx** files corresponding to malicious code. ScreenConnect does not place any files in this directory.

Sigma

```
title: ConnectWise ScreenConnect ZipSlip Exploitation (Feb 2024)
id: 4c198a60-7d05-4daf-8bf7-4136fb6f5c62
status: experimental
description: This detects file modifications to ASPX and ASHX files within the root of the App_Extensions
directory, which is allowed by a ZipSlip vulnerability in versions prior to 23.9.8.  This does occur during
exploitation of the vulnerability. This requires an Advanced Auditing policy to log a successful Windows
Event ID 4663 events and with a SACL set on the directory.
references:
  - https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
  - https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8
  - https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
author: Huntress DE&TH Team
date: 2024/02/20
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4663
    ObjectType: 'File'
    ProcessName|contains:
      - 'ScreenConnect.Service.exe'
    AccessMask: 0x6
  legitimate_path:
    ObjectName|endswith: 'ScreenConnect\App_Extensions\*\*'
  illegitimate_path:
    ObjectName|endswith: 'ScreenConnect\App_Extensions\*.as?x'
  condition: selection and illegitimate_path and not legitimate_path
falsepositives:
  - Unknown
level: critical
tags:
  - attack.initial_access
  - attack.persistence
```

Sources

- https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
- https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
- https://www.cve.org/CVERecord?id=CVE-2024-1709
- https://www.cve.org/CVERecord?id=CVE-2024-1708