Hive Pro®

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# Critical Vulnerabilities in ScreenConnect Under Active Exploitation

| Date of Publication | Last updated date | Admiralty Code | TA Number |
| --- | --- | --- | --- |
| February 22, 2024 | February 29, 2024 | A1 | TA2024072 |

# Summary

**First Seen:** February 13, 2024
**Affected Product:** ConnectWise ScreenConnect
**Malware:** LockBit Ransomware, BlackBasta Ransomware, Bl00dy Ransomware, Blackcat Ransomware, XWORM, and AsyncRAT
**Impact:** Critical vulnerabilities in ScreenConnect CVE-2024-1709 allow attackers unauthorized access without credentials, while CVE-2024-1708 enables remote code execution. Hackers can gain direct access to confidential information or critical systems. Immediate patching is essential to mitigate these threats and safeguard sensitive information.

## CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO -DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2024-1708 | ConnectWise ScreenConnect Path-Traversal Vulnerability | ConnectWise ScreenConnect | ✗ | ✗ | ✓ |
| CVE-2024-1709 | ConnectWise ScreenConnect Authentication Bypass Vulnerability | ConnectWise ScreenConnect | ✗ | ✓ | ✓ |

# Vulnerability Details

**#1**

ConnectWise issued emergency patches for two critical security flaws (CVE-2024-1709 and CVE-2024-1708) in its ScreenConnect remote desktop access product on February 19, 2024. Less than 24 hours later, hackers began exploiting these vulnerabilities to compromise enterprise accounts. The flaws include an authentication bypass and a path traversal bug, both rated with critical severity scores.

**#2**

The authentication bypass vulnerability (CVE-2024-1709) permits unauthorized access to the setup wizard, potentially granting administrative privileges. The path traversal flaw (CVE-2024-1708) could lead to ZipSlip attacks, enabling malicious extensions to write files anywhere within the ScreenConnect directory. Cloud instances have been remediated, but on-premise instances must upgrade to version 23.9.8 immediately.

**#3**

Attackers are capitalizing on CVE-2024-1709 to establish new administrative accounts and issue commands to upload malicious extensions and perform code execution by leveraging CVE-2024-1708. Shadow servers identified over 8200 vulnerable instances and observed 643 IPs exploiting CVE-2024-1709. Additionally, Metasploit has introduced an unauthenticated RCE exploit module, simplifying exploitation efforts.

**#4**

Numerous threat actors have been observed exploiting this vulnerability to deploy a range of malicious activities, including ransomware, infostealers, and Remote Access Clients. Among the malware variants utilized, XWORM and AsyncRAT stand out. In addition, the BlackBasta group and an unidentified entity have utilized this vulnerability to deploy Cobalt Strike beacons, while the Bl00dy ransomware group has leveraged leaked builders from both LockBit 3.0 and Conti in their operations. Blackcat resurged after a December 2023 disruption, causing disruptions at US pharmacies and the outage at a UnitedHealth Group unit, caused by exploiting CVE-2024-1709.

**#5**

These vulnerabilities specifically impact on-premises or self-hosted ScreenConnect customers utilizing versions 23.9.7 and earlier. These exploitation campaigns underscore the severity and broad-reaching impact of these vulnerabilities, necessitating immediate attention and mitigation efforts to safeguard systems and data from malicious attacks.

## Vulnerabilities

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2024-1708 | ScreenConnect 23.9.7 and prior | cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:* | CWE-22 |
| CVE-2024-1709 | ScreenConnect 23.9.7 and prior | cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:* | CWE-288 |

# Recommendations

**Apply Patches:** Ensure that all on-premise ScreenConnect installations are updated to version 23.9.8 or later, which includes patches for the identified vulnerabilities. Promptly install any future updates released by ConnectWise to address security issues and improve system resilience.

**Implement Access Controls:** Enforce strong authentication mechanisms, such as multi-factor authentication (MFA), to prevent unauthorized access to ScreenConnect instances. Limit access privileges to only necessary users and roles, reducing the attack surface and mitigating the impact of potential breaches.

**Secure Configuration:** Configure ScreenConnect servers and associated components securely based on vendor recommendations and industry best practices. Disable unnecessary services, ports, and features to reduce the likelihood of exploitation. Regularly review and update configurations to maintain security posture.

**Monitor for Suspicious Activity:** Implement robust logging and monitoring mechanisms to detect anomalous behavior and potential security incidents. Monitor system logs, network traffic, and user activities for signs of unauthorized access, privilege escalation, or exploitation attempts

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0011<br>Command and Control | TA0003<br>Persistence |
| TA0004<br>Privilege Escalation | TA0042<br>Resource Development | TA0010<br>Exfiltration | TA0007<br>Discovery |
| TA0040<br>Impact | T1105<br>Ingress Tool Transfer | T1068<br>Exploitation for Privilege Escalation | T1133<br>External Remote Services |
| T1588<br>Obtain Capabilities | T1059<br>Command and Scripting Interpreter | T1203<br>Exploitation for Client Execution | T1136<br>Create Account |
| T1486<br>Data Encrypted for Impact | T1055.012<br>Process Hollowing | T1055<br>Process Injection | T1059.001<br>PowerShell |

| | | | |
|---|---|---|---|
| T1087<br>Account Discovery | T1482<br>Domain Trust Discovery | T1041<br>Exfiltration Over C2 Channel | T1219<br>Remote Access Software |
| T1562<br>Impair Defenses | T1588.005<br>Exploits | T1588.006<br>Vulnerabilities | T1190<br>Exploit Public-Facing Application |
| T1078.003<br>Local Accounts | T1078<br>Valid Accounts | T1078.001<br>Default Accounts | T1087.003<br>Email Account |
| T1087.001<br>Local Account | | | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IPv4 | 155.133.5[.]15,<br>155.133.5[.]14,<br>118.69.65[.]60,<br>159[.]65[.]130[.]146 |
| SHA256 | 11d2dde6c51e977ed6e3f3d3e256c78062ae41fe780aefecfba1627e66daf771,<br>cc13b5721f2ee6081c1244dd367a9de958353c29e32ea8b66e3b20b293fabc55,<br>e3401d7699cc5067620e43bd24e8ccd437832c16f2fa7d5baaad8c170383cc92,<br>fa131238c3c35efe99cde59dd409c0436fd642b6bf5d56f994f52ab3a62bae4e,<br>764c53ea8ab98e4720ec55876c1b656d38e5e225c3835ffba491f64fa6b24b00,<br>3a659609850664cbc0683c8c7b92be816254eb9306e7fb12ad79d5a9af0fb623,<br>8e51de4774d27ad31a83d5df060ba008148665ab9caf6bc889a5e3fba4d7e600,<br>444338339260d884070de53554543785acc3c9772e92c5af1dff96e60e67c195,<br>47d83461ee57031fd2814382fb526937a4cfa9a3eea7a47e4e7ee185c0602b27,<br>f1c7045badec0b9771da4a0f067eac99587d235d1ede35190080cd051d923da |
| Domains | wipresolutions[.]com,<br>*.dns.artstrailreviews[.]com,<br>input-beats[.]gl[.]at[.]ply[.]gg,<br>scamkiller.duckdns[.]org |
| URLs | hxxp://23[.]26[.]137[.]225:8084/msappdata.msi,<br>hxxp://23[.]26[.]137[.]225:8091/chromeset.exe |

## Patch Details

- Upgrade ConnectWise ScreenConnect version to 23.9.8 or later versions.
- License restrictions have been removed, allowing all partners to upgrade.

Link:
https://screenconnect.connectwise.com/download

## References


https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass

https://github.com/rapid7/metasploit-framework/pull/18870

https://github.com/watchtowrlabs/connectwise-screenconnect_auth-bypass-add-user-poc

https://infosec.exchange/@SophosXOps/111975043941611370

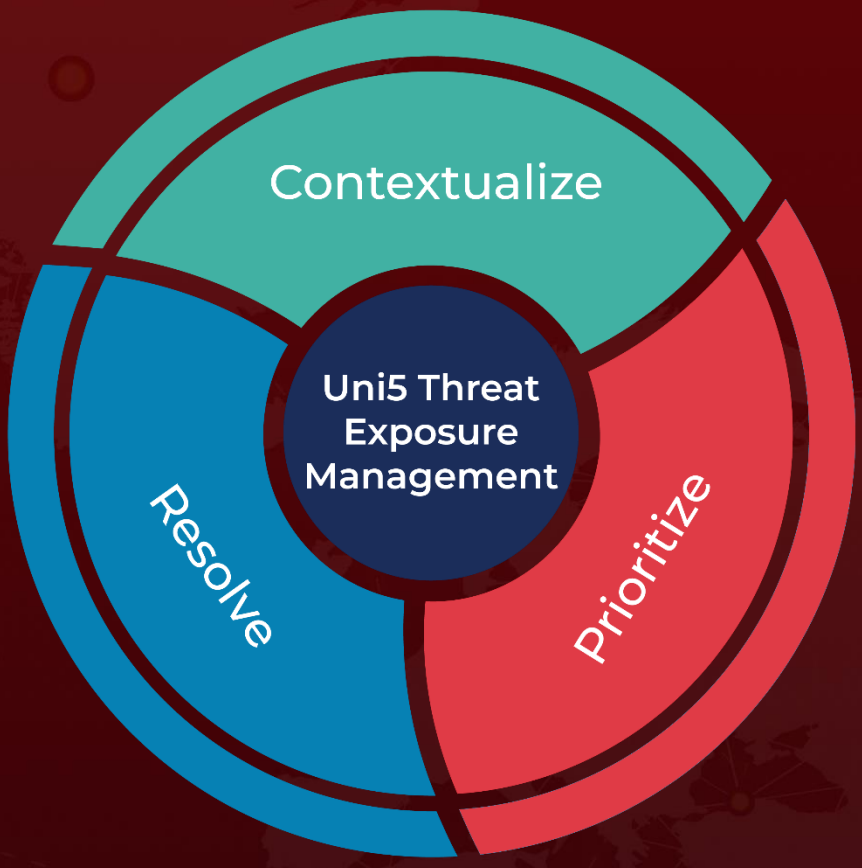
https://twitter.com/Shadowserver/status/1760740607268638809?s=20

https://www.trendmicro.com/en_us/research/24/b/threat-actor-groups-including-black-basta-are-exploiting-recent-.html

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**February 22, 2024 . 6:30 AM**



More at www.hivepro.com