February 22, 2024

Cyber Alert

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a ConnectWise ScreenConnect an authentication bypass and a path traversal vulnerability in versions prior to 23.9.8. ConnectWise has indicated that CVE-2024-1709 may be exploited in the wild.

Technical Details

On February 19, 2024, the Cyber Centre became aware of vulnerabilities impacting all versions of ConnectWise ScreenConnect prior to 23.9.8. In response, the Cyber Centre released advisory AV24-100 along with an update on February 20, 2024, highlighting that the vulnerabilities are being exploited.

ConnectWise reports that CVE-2024-1709 is an authentication bypass vulnerability and CVE-2024-1708 is a path traversal flaw. These vulnerabilities combined could allow for remote code execution (RCE).

While ConnectWise has indicated that CVE-2024-1709 may be exploited in the wild, open-source researchers have reported that exploitation impacting both CVE-2024-1708 and CVE-2024-1709 have been observed and in some cases resulted in the deployment of ransomware.

Suggested Action

The Cyber Centre strongly recommends that organizations patch any ScreenConnect systems immediately. ConnectWise recommends updating impacted products to version 23.9.8. The vendor states cloud partners are remediated against both vulnerabilities reported on February 19.

Organizations should also review and implement the Cyber Centre's Top 10 IT Security Actions with an emphasis on the following topics:

- Consolidating, monitoring, and defending Internet gateways.
- Patching operating systems and applications.
- Isolate web-facing applications.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-1708, CVE-2024-1709
- Unauthenticated Remote Code Execution in ConnectWise's ScreenConnect
- CCCS AV24-100 – ConnectWise Security Advisory
- ConnectWise – ConnectWise ScreenConnect 23.9.8 Security Fix
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- VRM Vulnerability Reports