Cutting Edge, Campaign C0029 | MITRE ATT&CK®

Archived: 2026-04-05 14:31:00 UTC

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

During Cutting Edge, threat actors used the publicly available Interactsh tool to identify Ivanti Connect Secure VPNs vulnerable to CVE-2024-21893.[5]

Enterprise T1071 .004 Application Layer Protocol: DNS

During Cutting Edge, threat actors used DNS to tunnel IPv4 C2 traffic.[4]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

During Cutting Edge, threat actors saved collected data to a tar archive.[4]

Enterprise T1059 Command and Scripting Interpreter

During Cutting Edge, threat actors used Perl scripts to enable the deployment of the THINSPOOL shell script dropper and for enumerating host data.[4][1]

.006 Python

During Cutting Edge, threat actors used a Python reverse shell and the PySoxy SOCKS5 proxy tool.[2][5]

Enterprise T1554 Compromise Host Software Binary

During Cutting Edge, threat actors trojanized legitimate files in Ivanti Connect Secure appliances with malicious code.[1][2][4]

Enterprise T1584 .008 Compromise Infrastructure: Network Devices

During Cutting Edge, threat actors used compromised and out-of-support Cyberoam VPN appliances for C2.[1][3]

Enterprise T1005 Data from Local System

During Cutting Edge, threat actors stole the running configuration and cache data from targeted Ivanti Connect Secure VPNs.[2][4]

Enterprise T1190 Exploit Public-Facing Application

During Cutting Edge, threat actors exploited CVE-2023-46805 and CVE-2024-21887 in Ivanti Connect Secure VPN appliances to enable authentication bypass and command injection. A server-side request forgery (SSRF) vulnerability, CVE-2024-21893, was identified later and used to bypass mitigations for the initial two vulnerabilities by chaining with CVE-2024-21887.[1][2][3][4][5]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

During Cutting Edge, threat actors disabled logging and modified the `compcheckresult.cgi` component to edit the Ivanti Connect Secure built-in Integrity Checker exclusion list to evade detection.[4][2]

Enterprise T1070 Indicator Removal

During Cutting Edge, threat actors cleared logs to remove traces of their activity and restored compromised systems to a clean state to bypass manufacturer mitigations for CVE-2023-46805 and CVE-2024-21887.[4][2]

.004 File Deletion

During Cutting Edge, threat actors deleted `/tmp/test1.txt` on compromised Ivanti Connect Secure VPNs which was used to hold stolen configuration and cache files.[4][5]

.006 Timestomp

During Cutting Edge, threat actors changed timestamps of multiple files on compromised Ivanti Secure Connect VPNs to conceal malicious activity.[4][5]

Enterprise T1105 Ingress Tool Transfer

During Cutting Edge, threat actors leveraged exploits to download remote files to Ivanti Connect Secure VPNs.[2]

Enterprise T1056 .001 Input Capture: Keylogging

During Cutting Edge, threat actors modified a JavaScript file on the Web SSL VPN component of Ivanti Connect Secure devices to keylog credentials.[2]

.003 Input Capture: Web Portal Capture

During Cutting Edge, threat actors modified the JavaScript loaded by the Ivanti Connect Secure login page to capture credentials entered.[2]

Enterprise T1095 Non-Application Layer Protocol

During Cutting Edge, threat actors used the Unix socket and a reverse TCP shell for C2 communications.[5]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

During Cutting Edge, threat actors used a Base64-encoded Python script to write a patched version of the Ivanti Connect Secure `dsls` binary.[4]

Enterprise T1588 .002 Obtain Capabilities: Tool

During Cutting Edge, threat actors leveraged tools including Interactsh to identify vulnerable targets, PySoxy to simultaneously dispatch traffic between multiple endpoints, BusyBox to enable post exploitation activities, and Kubo Injector to inject shared objects into process memory.[1][5]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

During Cutting Edge, threat actors used Task Manager to dump LSASS memory from Windows devices to disk.[2]

.003 OS Credential Dumping: NTDS

During Cutting Edge, threat actors accessed and mounted virtual hard disk backups to extract ntds.dit.[2]

Enterprise T1055 Process Injection

During Cutting Edge, threat actors used malicious SparkGateway plugins to inject shared objects into web process memory on compromised Ivanti Secure Connect VPNs to enable deployment of backdoors.[5]

Enterprise T1572 Protocol Tunneling

During Cutting Edge, threat actors used Iodine to tunnel IPv4 traffic over DNS.[4]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

During Cutting Edge, threat actors used RDP with compromised credentials for lateral movement.[2]

.002 Remote Services: SMB/Windows Admin Shares

During Cutting Edge, threat actors moved laterally using compromised credentials to connect to internal Windows systems with SMB.[2]

.004 Remote Services: SSH

During Cutting Edge, threat actors used SSH for lateral movement.[2]

Enterprise T1594 Search Victim-Owned Websites

During Cutting Edge, threat actors peformed reconnaissance of victims' internal websites via proxied connections.[2]

Enterprise T1505 .003 Server Software Component: Web Shell

During Cutting Edge, threat actors used multiple web shells to maintain presence on compromised Connect Secure appliances such as WIREFIRE, GLASSTOKEN, BUSHWALK, LIGHTWIRE, and FRAMESTING.[1][2]

Enterprise T1082 System Information Discovery

During Cutting Edge, threat actors used the ENUM4LINUX Perl script for discovery on Windows and Samba hosts.[4]

Enterprise T1205 Traffic Signaling

During Cutting Edge, threat actors sent a magic 48-byte sequence to enable the PITSOCK backdoor to communicate via the `/tmp/clientsDownload.sock` socket.[5]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

During Cutting Edge, threat actors used compromised VPN accounts for lateral movement on targeted networks. [2]
