Chinese Threat Group UNC5274 Reportedly Exploiting F5 BIG-IP and ScreenConnect CVEs for Active Exploitation - RH-ISAC

Published: 2024-03-22 · Archived: 2026-04-05 14:59:56 UTC

On March 21, 2023, Mandiant researchers reported their latest technical details detailing a campaign exploiting critical vulnerabilities in F5 BIG-IP and ScreenConnect, which they attribute to the Chinese state-sponsored actor known as UNC5174.

Community Impact Assessment

Due to the widespread use of F5 BIG-IP and ScreenConnect across global regions and industries, the RH-ISAC intelligence team assesses with moderate confidence that this campaign may pose a moderate threat to organizations that have not patched the critical flaws leveraged.

Additionally, given the historical targeting and methods leveraged, the RH-ISAC intelligence team assesses with moderate confidence that UNC5174 may pose a moderate threat to organizations in critical infrastructure sectors.

Members are advised to review the indicators of compromise (IOCs,) mitigations, detection rules, and MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) provided by Mandiant, included below.

Context and Technical Details

Mandiant reported that campaigns observed between October 2023 and February 2024 leveraged, respectively:

ConnectWise ScreenConnect Vulnerability CVE-2024-1709, a 10 CRITICAL severity vulnerability described thus: “ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.”

F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability CVE-2023-46747, a 9.8 CRITICAL severity vulnerability, described as thus: “Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands.”

According to Mandiant, the “mix of custom tooling and the SUPERSHELL framework […] is assessed with moderate confidence to be unique to a People’s Republic of China (PRC) threat actor, UNC5174 […] (believed to use the persona “Uteus”) is a former member of Chinese hacktivist collectives that has since shown indications of acting as a contractor for China’s Ministry of State Security (MSS) focused on executing access operations.”

“UNC5174 has been linked to widespread aggressive targeting and intrusions of Southeast Asian and U.S. research and education institutions, Hong Kong businesses, charities and non-governmental organizations (NGOs), and U.S. and UK government organizations during October and November 2023, as well as in February 2024.”

Mitigations

Mandiant provided the following remediation recommendations:

- Restrict access to the F5 TMUI from the internet.
- Immediately apply the F5 mitigation script published in **K000137353** to any vulnerable F5 appliances.
- Investigate vulnerable F5 appliances for evidence of compromise.

In the event of an F5 compromise:

- Review appliance configurations for unauthorized modifications.
- Review file system and operating system (OS) artifacts for evidence of privileged account creation and remove any unauthorized accounts.
- Consider revoking and re-issuing sensitive cryptographic material such as certificates and private keys that may have been accessible to a threat actor.

For impacted ScreenConnect instances, Mandiant recommends that organizations with an on-premises controller read the latest ScreenConnect remediation and hardening guide.

Detections

Mandiant provided the following detections:

rule M_Backdoor_GOREVERSE_2

{

meta:

author = “Mandiant”

description = “This rule is designed to detect events related to goreverse. GOREVERSE is a publicly available reverse shell”

md5 = “5c175ea3664279d6c0c2609844de6949”

platforms = “Windows,Linux,MacOS”

malware_family = “GOREVERSE”

strings:

$cc_main_fork_amd64 = { 41 81 39 74 72 75 65 75 ?? 48 8B [5] 48 8B [5] 48 8B [5] 4C 8B [5] 48 8B [5] 48 8B [5-10] E8 [4] 48 8B }

$cc_print_help_amd64 = { 48 8D 15 [4] 48 89 94 24 [4-16] 48 8B 1D [4] 48 8D 05 [4-24] BF 03 00 00 00 48 89 FE [0-12] E8 }

$cc_rssh = “rssh” fullword

```
        $cc_validate_dest_len = { 48 83 3D [4] 00 [1-24] 49 83 FC 01 [1-24] 49 C1 E4 05 [1-64] 83 3D [4] 00 }
        $str1 = "–[foreground|fingerprint|proxy|process_name] -d|–destination <server_address>"
        $str2 = "-d or –destination Server connect back address (can be baked in)"
        $str3 = "–foreground Causes the client to run without forking to background"
        $str4 = "–fingerprint Server public key SHA256 hex fingerprint for auth"
        $str5 = "–proxy Location of HTTP connect proxy to use"
        $str6 = "–process_name Process name shown in tasklist/process list"
    condition:
( ((uint32(0) == 0xcafebabe) or (uint32(0) == 0xfeedface) or (uint32(0) == 0xfeedfacf) or (uint32(0) == 0xbebafeca) or (uint32(0) == 0xcefaedfe) or (uint32(0) == 0xcffaedfe)) or (uint16(0) == 0x5a4d and uint32(uint32(0x3C)) == 0x00004550) or (uint32(0) == 0x464c457f)) and (all of ($str*) or all of ($cc_*))
}
rule M_APT_Downloader_SNOWLIGHT_1
{
    meta:
        author = "Mandiant"
        description = "This rule is designed to detect the SNOWLIGHT code family"
        md5 = "0951109dd1be0d84a33d52c135ba9c97"
        platforms = "Linux"
        malware_family = "SNOWLIGHT"
    strings:
        $xor99 = { 80 31 99 48 FF C1 89 CE 29 EE 39 C6 7C F2 48 63 D2 48 89 EE 44 89 E7 }
        $memfdcreate = { BA 01 00 00 00 BE 3B 0B 40 00 BF 3F 01 00 00 E8 8C FE FF FF }
    condition:
        uint32(0) == 0x464c457f and all of them
}
```

IOCs

Mandiant provided the following IOCs:

Indicator	Type	Notes
hxxp://172.245.68[.]110:8888	URL	SUPERSHELL C2
172.245.68[.]110	IP Address	Colocrossing
61.239.68[.]73	IP Address	Hong Kong Broadband Network Ltd.
118.140.151[.]242	IP Address	HGC Global Communications Limited
c867881c56698f938b4e8edafe76a09b	MD5	SNOWLIGHT
df4603548b10211f0aa77d0e9a172438	MD5	SNOWLIGHT
0951109dd1be0d84a33d52c135ba9c97	MD5	SNOWLIGHT
9c3bf506dd19c08c0ed3af9c1708a770	MD5	N/A
0ba435460fb7622344eec28063274b8a	MD5	SNOWLIGHT
a78bf3d16349eba86719539ee8ef562d	MD5	SNOWLIGHT

TTPs

Mandiant provided the following TTPs:

Technique	Number	Description
Initial Access	T1190	Exploit Public-Facing Application

Defense Evasion	T1027	Obfuscated Files or Information
	T1070.004	File Deletion
	T1140	Deobfuscate/Decode Files or Information
	T1222.002	Linux and Mac File and Directory Permissions Modification
	T1601.001	Patch System Image
Discovery	T1016	System Network Configuration Discovery
	T1049	System Network Connections Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Command and Control	T1095	Non-Application Layer Protocol
	T1105	Ingress Tool Transfer
	T1572	Protocol Tunneling
	T1573.002	Asymmetric Cryptography
Execution	T1059	Command and Scripting Interpreter
	T1059.004	Unix Shell

Persistence	T1136.001	Local Account
Impact	T1531	Account Access Removal
Credential Access	T1003.008	/etc/passwd and /etc/shadow
Resource Development	T1608.003	Install Digital Certificate
