Active Exploitation of Mitel SIP Phone Vulnerability by Aquabot DDoS Botnet

TL;DR

A Mirai-based botnet known as Aquabot is actively exploiting a known command injection vulnerability (CVE-2024-41710) in Mitel SIP phones to pull exposed devices into DDoS operations. The issue was patched in mid-2024, but unpatched phones are now being targeted in attacks.

Overview

Attackers are now exploiting CVE-2024-41710 (CVSS 6.8) in exposed Mitel SIP phones. The activity ties back to Aquabot, a Mirai-based botnet that's been around since late 2023 and is being used for DDoS attacks.

The flaw allows attackers to inject system-level commands into the phone's local configuration during the boot process by sending specially crafted HTTP requests to exposed management endpoints. Successful exploitation gives the attacker full control of the device. While Mitel patched the issue in July 2024, exploitation activity increased after a public proof-of-concept was released in August, and attacks were observed beginning in early January 2025.

Affected devices include:

- Mitel 6800 Series SIP Phones
- Mitel 6900 Series and 6900w Series SIP Phones
- Mitel 6970 Conference Unit

Devices running R6.4.0.HF1 (R6.4.0.136) and earlier are vulnerable.

Once compromised, devices are not used for surveillance or data theft. They are absorbed into a botnet and controlled through external command-and-control infrastructure for distributed denial-of-service attacks. The Aquabot variant observed in this campaign includes behavior not previously seen in Mirai-based malware, including monitoring for termination signals and reporting attempted kill actions back to its C2 server.

The malware also renames itself to resemble legitimate system processes and terminates local shells or competing malware to maintain control of the device. In addition to Mitel phones, Aquabot has been observed exploiting other widely abused IoT and network service vulnerabilities. VoIP phones are frequently overlooked and left

exposed, which makes them easy targets for DDoS attacks. Due to exploitation, Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Patch all affected Mitel SIP phones and conference units to versions that address CVE-2024-41710. See Mitel's advisory for details.
- Confirm that phone management interfaces are not exposed directly to the internet
- Restrict administrative access to VoIP devices using firewall rules and network segmentation
- Monitor VoIP and IoT devices for unusual outbound traffic patterns

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may have exploited CVE-2024-41710 by sending crafted HTTP requests to exposed Mitel phone management endpoints to execute commands during the boot process.

Command and Control

- Application Layer Protocol [T1071.001] – The compromised devices may have established outbound connections to external C2 infrastructure to receive instructions and report status.

Impact

- Network Denial of Service [T1498] – The attacker may have used the compromised phones as part of a Mirai-based botnet to generate DDoS traffic.

IoCs

IP Addresses

- 89[.]190[.]156[.]145
- 193[.]200[.]78[.]33
- 173[.]239[.]233[.]46
- 173[.]239[.]233[.]47
- 173[.]239[.]233[.]48

- 141[.]98[.]11[.]67
- 141[.]98[.]11[.]175

Domains

- intenseapi[.]com
- eye-network[.]ru
- dogmuncher[.]xyz
- cloudboats[.]vip
- theeyefirewall[.]su

Suspicious Filenames and Process Names

- Aqua.x86
- Aqua.arm
- Aqua.mips
- httpd.x86

Targeted Industries

This activity impacts organizations using Mitel SIP phones and conference units, particularly where devices are internet-reachable or lightly monitored.

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

- Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Active Exploitation: New Aquabot Variant Phones Home | Akamai
Mitel Product Security Advisory 24-0019 | Mitel
NVD - CVE-2024-41710