مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Mitel SIP Phones

Tracking #:432317249

Date:12-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two significant vulnerabilities have been identified in Mitel SIP phone product lines, including the 6800, 6900, 6900w Series, and the 6970 Conference Unit.

TECHNICAL DETAILS:

Two vulnerabilities (CVE-2025-47188 and CVE-2025-47187) affecting Mitel 6800, 6900, 6900w Series SIP Phones, and the 6970 Conference Unit pose significant risks to organizational security. The critical command injection flaw (CVSS 9.8) allows unauthenticated attackers to execute arbitrary commands, potentially compromising sensitive data and device functionality. A secondary file upload vulnerability (CVSS 5.3) enables storage exhaustion attacks.

Vulnerability Details

1. **CVE-2025-47188: Command Injection (CVSS 9.8 – Critical)**
   - **Cause**: Insufficient sanitization of user-supplied parameters
   - **Impact**: Enables unauthenticated attackers to execute arbitrary commands, leading to:
     - Disclosure/modification of system and user configurations.
     - Full device compromise (root access) and potential VoIP infrastructure disruption

2. **CVE-2025-47187: Unauthenticated File Upload (CVSS 5.3 – Medium)**
   - **Cause**: Improper authentication mechanisms for file uploads
   - **Impact**: Allows attackers to upload arbitrary WAV files, exhausting device storage and potentially enabling secondary attacks

Affected Products:

Product Series	Affected Firmware	Patched Version
6800 Series SIP Phones	R6.4.0.SP4 and earlier	R6.4.0.SP5+
6900 Series SIP Phones	R6.4.0.SP4 and earlier	R6.4.0.SP5+
6900w Series SIP Phones	R6.4.0.SP4 and earlier	R6.4.0.SP5+
6970 Conference Unit	R6.4.0.SP4 and earlier	R6.4.0.SP5+

RECOMMENDATIONS:

- Upgrade all affected Mitel SIP devices to fixed firmware version R6.4.0.SP5 or later.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.mitel.com/support/mitel-product-security-advisory-misa-2025-0004