July 18, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of Mitel published security advisories to address vulnerabilities in the following products:

- Mitel 6800 Series SIP Phones – version R6.4.0.HF1 (R6.4.0.136) and prior
- Mitel 6900 Series SIP Phones – version R6.4.0.HF1 (R6.4.0.136) and prior
- Mitel 6900w Series SIP Phones – version R6.4.0.HF1 (R6.4.0.136) and prior
- Mitel 6970 Conference Unit – version R6.4.0.HF1 (R6.4.0.136) and prior
- Unify OpenScape 4000 – version v11 R0.22 and prior
- Unify OpenScape 4000 Assistant – version v11 R0.22 and prior
- Unify OpenScape 4000 Manager – versions v10 R1.34, V10 R1.42 and v11 R0.22 and prior

.

Technical Details

A command injection vulnerability in the Platform Webservice component of Unify OpenScape 4000 and Unify OpenScape 4000 Manager, could allow an unauthenticated attacker to conduct a command injection attack due to insufficient parameter sanitization. A successful exploit of this vulnerability could allow an attacker to execute arbitrary commands within the context of the system, with a potential impact on the confidentiality, integrity, and availability of the system.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- **Mitel security advisory - 24-0019**
- **Mitel security advisory - 24-0020**
- **Mitel security advisory - OBSO-2407-02**
- **Mitel security advisory - OBSO-2407-03**
- **Mitel Security Advisories**