Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Flaws in Mitel MiCollab: Path Traversal and SQL Injection Risks Unveiled

Date of Publication	Admiralty Code	TA Number
January 8, 2025	A1	TA2025006

Summary

First Seen: October 2024
Affected Products: Mitel MiCollab
Impact: Critical security vulnerabilities CVE-2024-41713, CVE-2024-55550, and CVE-2024-35286 have been uncovered in Mitel MiCollab, exposing organizations to significant risks. These flaws could allow attackers to bypass authentication and access files on affected servers, potentially revealing sensitive data and compromising system security. Exploiting these vulnerabilities could lead to unauthorized access, endangering the confidentiality, integrity, and availability of impacted systems. Furthermore, CVE-2024-41713 and CVE-2024-35286 can be chained together for more advanced attacks, enabling threat actors to compromise systems, steal sensitive information, and disrupt enterprise operations.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-41713	Mitel MiCollab Path Traversal Vulnerability	Mitel MiCollab	✗	✓	✓
CVE-2024-55550	Mitel MiCollab Path Traversal Vulnerability	Mitel MiCollab	✗	✓	✓
CVE-2024-35286	Mitel MiCollab SQL Injection Vulnerability	Mitel MiCollab	✗	✗	✓

Vulnerability Details

#1 Multiple security vulnerabilities have been discovered in Mitel MiCollab, including CVE-2024-41713, CVE-2024-55550, and CVE-2024-35286, putting organizations at serious risk. These flaws could allow attackers to bypass authentication mechanisms, access sensitive files, and compromise the overall security of affected systems. Exploitation of these vulnerabilities may lead to unauthorized access, threatening the confidentiality, integrity, and availability of enterprise infrastructure.

#2 CVE-2024-41713 is a path traversal vulnerability within the NuPoint Unified Messaging (NPM) component of Mitel MiCollab. This flaw arises from insufficient input validation, enabling unauthenticated attackers to conduct path traversal attacks. If exploited, attackers could gain unauthorized access to provisioning information, such as user and network data, and perform unauthorized administrative actions on the MiCollab server, all without requiring authentication.

#3 CVE-2024-55550 is another path traversal vulnerability that affects Mitel MiCollab. Unlike CVE-2024-41713, this flaw requires administrative privileges for exploitation. An authenticated attacker with admin access could exploit insufficient input sanitization to read local files within the system. However, the impact is limited to non-sensitive system information, without the ability to modify files or escalate privileges.

#4 CVE-2024-35286 is a SQL injection vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab. This flaw, if successfully exploited, could enable attackers to inject malicious SQL commands, compromising the database and gaining unauthorized access to sensitive information. Notably, CVE-2024-41713 and CVE-2024-35286 can be chained together to execute advanced attacks. Proof-of-concept (PoC) exploits have demonstrated how this combination can allow attackers to bypass security layers, exfiltrate sensitive data, and disrupt operations. This exploit chain highlights the critical danger of seemingly limited vulnerabilities when combined, amplifying their impact on enterprise security.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-41713	MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*:*	CWE-22
CVE-2024-55550	MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*:*	CWE-22
CVE-2024-35286	MiCollab Version 9.8.0.33 and earlier	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*:*	CWE-89

Recommendations

Apply Patch: Upgrade to the latest version of Mitel MiCollab as recommended by Mitel to address CVE-2024-41713, CVE-2024-55550, and CVE-2024-35286. Ensure all security patches are applied promptly.

Restrict Access: Limit access to the Mitel MiCollab management interface to trusted IP ranges. Use network segmentation and firewalls to reduce exposure to untrusted users.

Monitor for Anomalies: Deploy security monitoring tools to detect unusual activity on the Mitel MiCollab servers. Monitor logs for signs of path traversal, SQL injection attempts, or unauthorized administrative actions.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0007** Discovery	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1078** Valid Accounts	**T1016** System Network Configuration Discovery	**T1083** File and Directory Discovery

Patch Details

Promptly update to latest version of Mitel MiCollab Version 9.8 SP2 (9.8.2.12) or later., as this version includes the necessary patch to address the vulnerabilities.

Links:
https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029

https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin240014001-v10.pdf

References

https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029

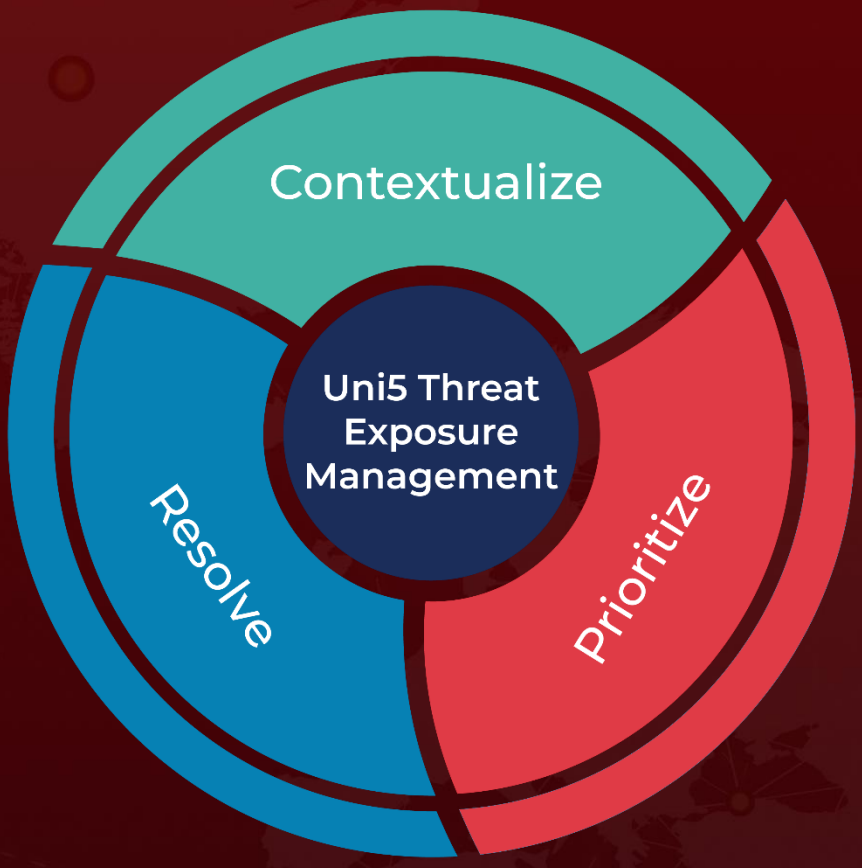
https://socradar.io/mitel-micollab-poc-exploit-cve-2024-41713-and-zero-day/

https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0014

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 8, 2025 . 6:00 AM

More at www.hivepro.com