



# NCSC-2024-0468

## Kwetsbaarheden verholpen in Mitel MiCollab

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-12-2024

### **TLP:WHITE**

#### **Toegestane verspreiding van TLP:WHITE**

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First ([www.first.org/tlp](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Mitel heeft kwetsbaarheden verholpen in Mitel MiCollab (Specifiek voor de Unified Messaging en Conferencing componenten).

## Duiding

De kwetsbaarheden bevinden zich in de manier waarop de Mitel MiCollab componenten omgaan met gebruikersinvoer. Een aanvaller kan deze kwetsbaarheden misbruiken om ongeautoriseerde toegang te krijgen tot gebruikersdata en systeemconfiguraties via path traversal en SQL-injectie aanvallen. Bovendien kunnen aanvallers phishing-aanvallen uitvoeren door middel van CRLF-injectie. Een proof-of-concept exploit is openbaar gemaakt, wat de haalbaarheid van deze aanvallen aantoont. De kwetsbaarheden zijn ernstig en kunnen leiden tot datalekken en compromittering van de integriteit van het systeem.

## Oplossingen

Mitel heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0025>
- <https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0026>
- <https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0027>
- <https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0028>
- <https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029>

## Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-41713	7.5 HIGH
➤ CVE-2024-47189	7.7 HIGH
➤ CVE-2024-47223	9.4 CRITICAL
➤ CVE-2024-47224	
➤ CVE-2024-47912	8.2 HIGH

## CWE's

CWE	Beschrijving
> <a href="#">CWE-93</a>	Improper Neutralization of CRLF Sequences ('CRLF Injection')
> <a href="#">CWE-116</a>	Improper Encoding or Escaping of Output
> <a href="#">CWE-306</a>	Missing Authentication for Critical Function
> <a href="#">CWE-284</a>	Improper Access Control
> <a href="#">CWE-89</a>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## Getroffen producten

<b>mitel</b>
micollab
mitel_micollab__9.8_sp2__9.8.2.12_

## Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.