Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0514

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Mitel MiCollab

Publicatiedatum: 24-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Mitel heeft meerdere kwetsbaarheden verholpen in Mitel MiCollab, specifiek in de Audio, Web en Video Conferencing component, voor versies tot en met 10.3.0.18.

Duiding

De kwetsbaarheden bevinden zich in de Audio, Web en Video Conferencing component van Mitel MiCollab.

Ongeauthenticeerde aanvallers kunnen door onvoldoende validatie van geüploade bestandstypen willekeurige bestanden uploaden, wat kan leiden tot het uitvoeren van kwaadaardige code of verstoring van systeemprocessen. Daarnaast kunnen zij XML-injectie aanvallen uitvoeren door gebruik te maken van vooraf geplaatste kwaadaardige inhoud, waarmee zij willekeurige commando's op het onderliggende systeem kunnen uitvoeren. Verder maakt een gebrek aan juiste inputsanitisatie blind command injection mogelijk, waardoor ook zonder authenticatie commando's uitgevoerd kunnen worden.

Ook is er een kwetsbaarheid die het mogelijk maakt om zonder authenticatie toegang te krijgen tot gevoelige informatie binnen bepaalde functionaliteiten van de conferencing component. Ten slotte kan door onjuiste authenticatieafhandeling een bypass van authenticatiecontroles plaatsvinden, waardoor onbevoegde acties binnen het systeem mogelijk zijn.

Deze kwetsbaarheden zijn specifiek van toepassing op versies tot en met 10.3.0.18 van Mitel MiCollab.

Oplossingen

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

Referenties

- https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2026-0012

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-133275	5.3 MEDIUM
CVE-2026-133303	9.0 CRITICAL
CVE-2026-133311	5.9 MEDIUM
CVE-2026-133323	10.0 CRITICAL
CVE-2026-133324	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-91	XML Injection
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-636	Not Failing Securely
CWE-1390	Weak Authentication

Getroffen producten

Mitel
MiCollab

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.