Mitel Product Security Advisory MISA-2025-0004

Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit Command Injection and Unauthenticated File Upload Vulnerabilities

Advisory ID:	MISA-2025-0004
Publish Date:	2025-05-07
Last Updated:	2025-05-07
Revision:	1.0

Summary

A command injection vulnerability, CVE-2025-47188, has been identified in the 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, which if successfully exploited 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 phone leading to disclosure or modification of sensitive system and user configuration data, and potentially affecting device availability and operation. The vulnerability severity is rated as critical.

An unauthenticated file upload vulnerability, CVE-2025-47187, has been identified in the 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, which if successfully exploited could allow an unauthenticated attacker to conduct a file upload attack due to improper authentication mechanisms. A successful exploit of this vulnerability could allow an attacker to upload arbitrary WAV files, which may potentially exhaust the phone’s storage without affecting the phone's availability or operation. The vulnerability severity is rated as medium.

A successful exploit of these vulnerabilities requires network access to the phone, which based on Mitel engineering guidelines should be deployed on a protected internal network.

The vulnerability severity for this security advisory is rated as critical.

Mitel is recommending customers with affected product versions update to the highlighted fixes. For customers that are unable to update in a timely manner Mitel recommends reviewing available workarounds.

Credit is given to Marc Bollhalder of InfoGuard Labs for highlighting these issues and bringing them to our attention.

Affected Products and Solutions

This security advisory provides information on the following products:

PRODUCT NAME	VERSION(S) AFFECTED	SOLUTION(S) AVAILABLE
Mitel 6800 Series SIP Phones	R6.4.0.SP4 and earlier	Upgrade to version R6.4.0.SP5 or later
Mitel 6900 Series SIP Phones	R6.4.0.SP4 and earlier	Upgrade to version R6.4.0.SP5 or later
Mitel 6900w Series SIP Phone	R6.4.0.SP4 and earlier	Upgrade to version R6.4.0.SP5 or later
Mitel 6970 Conference Unit	R6.4.0.SP4 and earlier	Upgrade to version R6.4.0.SP5 or later

Product statements are related only to supported product versions. Products which have reached End of Support status are not considered.

Vulnerability Severity

The following products have been identified as affected:

PRODUCT NAME	CVE ID	SEVERITY	CVSS 3.1 BASE SCORE
Mitel 6800 Series SIP Phones	CVE-2025-47188	9.8 (Critical)	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Mitel 6900 Series SIP Phones	CVE-2025-47188	9.8 (Critical)	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Mitel 6900w Series SIP Phone	CVE-2025-47188	9.8 (Critical)	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Mitel 6970 Conference Unit	CVE-2025-47188	9.8 (Critical)	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Mitel 6800 Series SIP Phones	CVE-2025-47187	5.3 (Medium)	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Mitel 6900 Series SIP Phones	CVE-2025-47187	5.3 (Medium)	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Mitel 6900w Series SIP Phone	CVE-2025-47187	5.3 (Medium)	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Mitel 6970 Conference Unit	CVE-2025-47187	5.3 (Medium)	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

The identified vulnerabilities carry varied levels of severity, ranging from critical to medium.

Mitigations / Workarounds

The risk may be mitigated by following the instructions found in the KMS article.

Solution/ Recommended Action

These issues are corrected in Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit, versions R6.4.0.SP5 or later. Customers are advised to update to this or a subsequent release.

Please see Mitel Knowledge Base article SO8496, “Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit Security Update, CVE-2025-47187 and CVE-2025-47188” https://mitel.custhelp.com/app/answers/answer_view/a_id/1021663.

If you do not have access to these links, please contact your Mitel Authorized Partner for support.

For further information, please contact Mitel Product Support.

For Open SIP customers, please contact Open SIP Support at sipphonesupport@mitel.com.

References

- CVE-2025-47188
- CVE-2025-47187

Revision History

Version	Date	Description
1.0	2025-05-07	Initial release

Publisher and Legal Disclaimer

Publisher: Mitel PSIRT / psirt@mitel.com

The information provided in this advisory is provided "as is" without warranty of any kind. The information is subject to change without notice. Mitel and its affiliates do not guarantee and accept no legal liability whatsoever arising from or connected to the accuracy, reliability, currency or completeness of the information provided. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.