# MNDT-2022-0037

## Description

Avaya IP Office for Windows contains a local privilege escalation vulnerability which affected version 11.1 FP2 SP1 and earlier.

## Impact

High - Exploiting the vulnerability will give a local unprivileged attacker SYSTEM level privileges.

## Exploitability

Medium - Any authenticated local user can exploit the vulnerability and an exploit is trivial to produce.

## CVE Reference

CVE-2021-25657

## Common Weakness Enumeration

CWE-379: Creation of Temporary File in Directory with Insecure Permissions

## Common Vulnerability Scoring System

Base Score: 7.8 - Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## Technical Details

The installation of the agent uses the Windows Installer framework and an MSI file is cached in c:\windows\installer. An unprivileged user can trigger a repair operation, either by using the Windows Installer API or by running "msiexec.exe /fa c:\windows\installer\[XXXXX].msi".

Running a repair operation will trigger a number of file operations in the %TEMP% folder of the user triggering the repair. Some of these operations will be performed from a SYSTEM context (started via the Windows Installer service), including the execution of temporary files.

## Resolution

The issue was fixed with the 11.1 Feature Pack 2 Service Pack 2 or later July 2022 Critical Patch Update. Update to address the vulnerability.

## Discovery Credits

- Ronnie Salomonsen, Mandiant

## Disclosure Timeline

- 30-Sep-2021 - Issue reported to Avaya
- 30-Nov-2021 - Issue confirmed by Avaya and a fix scheduled for March 17, 2022.
- 17-Mar-2022 - Patched version released by Avaya

## References

- Avaya Security Advisory
- Mitre CVE-2021-25657