



CVE-2018-18567

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-18567
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-24 22:29:00 UTC
Updated	2018-12-07 17:37:00 UTC
Description	AudioCodes 440HD and 450HD devices 3.1.2.89 and earlier allows man-in-the-middle attackers to obtain sensitive credent

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Audiocodes	440hd	-	All	All	All
Hardware	Audiocodes	440hd	-	All	All	All
Operating System	Audiocodes	440hd Firmware	All	All	All	All
Hardware	Audiocodes	450hd	-	All	All	All
Hardware	Audiocodes	450hd	-	All	All	All
Operating System	Audiocodes	450hd Firmware	All	All	All	All

References

Reference	Source
Microsoft Skype for Business Audio File Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECURITY
www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2018-026.txt	MISC
Bugtraq: [SYSS-2018-026] missing X.509 validation with AudioCodes IP Phones (Skype for Business, on-premise) - CVE-2018-18567	BUG
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)