SECURITY ADVISORIES–Yealink IP Phone WEB Server Vulnerabilities

CVE Dictionary Entry:CVE-2018-16221

CVE Dictionary Entry:CVE-2018-16218

CVE Dictionary Entry:CVE-2018-16217

DATE PUBLISHED: 2019-05-29

Please Note: Yealink takes the security of our customers and our products seriously. This is a living document and may be subject to updates. The latest version of this document can be found at the following URL: *https://www.yealink.com/trust-center-resource*

Vulnerability Summary

The diagnostics web interface in the Yealink Ultra-elegant IP Phone SIP-T41P (firmware 66.83.0.35) does not validate (escape) the path information (path traversal), which allows an authenticated remote attacker to get access to privileged information (e.g., /etc/passwd) via path traversal (relative path information in the file parameter of the corresponding POST request).

Solution

Yealink has released software updates to all affected phone models that contain fixes for these issues as well as other fixes and features. Please refer to the release notes for your particular endpoint for more information.

Phone Series：

Product Family and Model	Fixed Software Release
SIP-T27P	45.83.0.120
SIP-T29G	46.83.0.120
SIP-T41P	36.83.0.120
SIP-T42G	29.83.0.120
SIP-T46G	28.83.0.120
SIP-T48G	35.83.0.120
SIP-T19P_E2	53.84.0.130
SIP-T21P_E2	52.84.0.130
SIP-T23G	44.84.0.130
SIP-T40P	54.84.0.130
SIP-T40G	76.84.0.130
SIP-T52S/T54S	70.84.0.80

SIP-CP920	78.86.0.15
T4XS Series Phones	66. 86.0.15
T4XU Series Phones	108.86.0.60
T3X Series Phones	124.86.0.60
T5X Series Phones	96.86.0.60
SIP-T58	58.86.0.5
SIP-CP960	73.86.0.5
SIP-VP59	91.86.0.5
SIP-T58W	150.86.0.35
SIP-CP965	143.86.0.5
VP59-Zoom	91.30.0.30
MP5X-Zoom	122.30.0.15
MP5X-Teams	122.15.0.9
T5X-Teams	58.15.0.53
CP960-Teams	73.15.0.163
CP965-Teams	143.15.0.12

VCS Series :

Product Family and Model	Fixed Software Release
VC210 Series	118.320.0.15
MeetingEye400 Series	120.320.0.15
MeetingEye400Pro Series	133.320.0.15
MeetingEye800 Series	129.320.0.30
VP59-VCS	91.353.0.10
CTP18	137.353.0.15
MeetingBarA20/A30	133.15.0.105
MeetingBoard65	155.310.0.15
RoomPanel	147.15.0.33
RoomCast	144.312.0.5

The software, release notes, and other documentation for your voice endpoint can be found at: https://support.yealink.com/en/portal/home

Mitigation

Yealink recommends all customers upgrade to the latest version.

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Yealink Technical Support by visiting: https://support.yealink.com/en/portal/home *for the latest information.*

You might also find value in the high-level security guidance and security news located at:
https://support.yealink.com/en/portal/home