More Vulnerabilities in Poly IP Phones

Researchers of the Competence Center for IT-Security at the FZI Research Center for Information Technology found further vulnerabilities in Poly IP Phones. More precisely, the models VVX 410 and VVX 411 are affected. This advisory demonstrates that the mitigations introduced in response to the vulnerability FZI-2019-3 published in our advisory from the 15th of October 2019 are not effective. The vulnerability is part of the BToE functionality that allows to pair the phone with Skype for Business. It can be used by an attacker to wiretap a phone over the network. We disclosed the vulnerabilities to Poly according to our disclosure policy.

1 Vulnerabilities

1.1 Unauthenticated Access to BToE Service

The phone allows unauthenticated access to the BToE service over the network. An attacker can use the service to wiretap the phone. The vulnerability has been fixed partially by UC Software 6.2.0.3937. The phone requires a valid pairing code when connecting via TLS in the manual pairing mode. However, connecting via the legacy SSH protocol, which is enabled by default, does not require a pairing code to connect to the phone. Thus, this version is still susceptible.

FZI-ID	FZI-2019-3
CVE	CVE-2020-12871
Manufacturer	Poly
Product	VVX 410, VVX 411
Affected Version	VVX 410: 5.9.4.3247, VVX411: 6.2.0.3937
Type	CWE-287 - Improper Authentication
Date Found	17.07.2018
Patch Available	Incomplete
Patch Version	VVX 411: 6.2.0.3937
CVSS Score	6.5
CVSS String	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:L

1.2 Passcode Brute-force

In manual pairing mode, a pairing code is necessary to pair the BToE connector application with the phone. The pairing code encodes the IPv4 address of the phone. For each IP address, there are only 65536 possible pairing codes, which can be exploited by a brute-force attack. The phone does not limit the number of failed authentication attempts and thus an attacker can identify the correct pairing code quickly. After determining the correct pairing code, an attacker can activate the microphone via the BToE protocol and thereby wiretap the phone.

FZI-ID	FZI-2020-1
CVE	CVE-2020-13635
Manufacturer	Poly
Product	VVX 410, VVX 411
Affected Version	VVX 410: 5.9.5.0614, VVX 411: 6.2.0.3937
Type	CWE-307 - Improper Restriction of Excessive Authentication Attempts
Date Found	28.01.2020
Patch Available	Unverified
Patch Version	VVX 411: 6.3.0
CVSS Score	6.5
CVSS String	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:L

1.3 Authentication Bypass in Automatic Pairing Mode

Starting from UC Software 6.2.0.3937 the phone requires a pairing code message upon connection establishment to access the BToE functionality. In the automatic pairing mode, instead of the pairing code a secret value is used. The secret is derived from the IP address of the phone and can be generated by an attacker. Similar to the pairing code, there are several possible secrets for each IP address. Using a fake secret, the BToE functionality in automatic pairing mode can be accessed by an attacker and thus the phone can be wiretapped.

FZI-ID	FZI-2020-2
CVE	CVE-2020-13636
Manufacturer	Poly
Product	VVX 411
Affected Version	6.2.0.3937
Type	CWE-287 - Improper Authentication
Date Found	28.01.2020
Patch Available	Unverified
Patch Version	6.3.0
CVSS Score	6.5
CVSS String	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:L

2 Mitigation

UC Software 6.3.0 is supposed to fix CVE-2020-13635 and CVE-2020-13636. However, at the time of writing, UC Software 6.3.0 has not been released yet. For CVE-2020-12871 a patch is planned but no version or release date is known. The vulnerabilities can be mitigated by disabling the BToE functionality with the following configuration.

```
feature.btoe.enabled="0"
```

Configuration to disable BToE.

3 Disclosure Timeline

- 12.02.2020: Report of vulnerabilities to Poly
- 12.02.2020: Acknowledgment of receipt
- 14.04.2020: Notification from Poly that the vulnerabilities are addressed by UC Software 6.3.0, 5.9.7 and 6.4.0
- 12.05.2020: Extension of the deadline until 18.05.2020 due to the difficult current working situation
- 15.05.2020: Request by Poly to postpone publication until UC Software 6.3.0 is available which is supposed to fix CVE-2020-13635 and CVE-2020-13636 at the end of May
- 18.05.2020: Extension of the deadline until 08.06.2020 because a patch for two of the vulnerabilities is scheduled
- 21.05.2020: Poly reports CVE-2020-12871
- 05.06.2020: Poly reports CVE-2020-13635 and CVE-2020-13636
- 08.06.2020: Publication