Multiple Vulnerabilities in Poly IP Phones

Researchers of the Competence Center for IT-Security at the FZI Research Center for Information Technology found multiple vulnerabilities in the Poly VVX 410 and VVX 411 IP phones and the associated Better Together over Ethernet (BToE) connector application. These vulnerabilities could be used to leak domain credentials of users, wiretap a phone and possibly to execute arbitrary code. Three of the following four vulnerabilities are related to the BToE functionality that can be used to pair the phone with Skype for Business. We disclosed the vulnerabilities to Poly according to our responsible disclosure policy. Because the deadline passed, we publish details of the vulnerabilities.

1 Vulnerabilities

1.1 Unauthenticated Leak of Credentials in BToE Connector

The BToE connector application, which is necessary to pair the phone with Skype for Business, does not authenticate the remote end when initiating a connection. An attacker can exploit this to trigger a login prompt and leak entered credentials. Poly published a security advisory for this vulnerability and registered it as CVE-2019-10689. To mitigate the vulnerability update the phone to UC Software 5.9.3 (VVX 410) or 6.0.0 (VVX 411) and the BToE connector application to version 4.0.0.0. However, because of downward compatibility an additional workaround is necessary to fix the vulnerability. The workaround is to remove the file *plink.exe* from the program directory.

ID	FZI-2019-1
Manufacturer	Poly
Product	BToE Connector
Affected Version	<= 4.2.0.0
Patch	Incomplete (BToE Connector >= 4.0.0.0)
CVSS Score	5.9
CVSS String	CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L

1.2 Buffer Overflow in BToE Service

Due to a missing length check, the BToE service of the phone suffers from a remote buffer overflow vulnerability, which could result in denial of service and the execution of arbitrary code. The vulnerability can be triggered from the network without any prior authentication.

ID	FZI-2019-2
Manufacturer	Poly
Product	VVX 410, VVX 411
Affected Version (VVX 410)	UC Software <= 5.9.3.2857
Affected Version (VVX 411)	UC Software <= 6.1.0.6189
Patch (VVX 410)	Patched (UC Software 5.9.4)
Patch (VVX 411)	-
CVSS Score	4.8
CVSS String	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L

1.3 Unauthenticated Access to BToE Service

The phone does not require any authentication to access the BToE service. An attacker can exploit this vulnerability over the network without any prior authentication to wiretap the phone. Note that the pairing code in the manual pairing mode does not prevent the attack. To mitigate the vulnerability, disable BToE until a patch from the manufacturer is available.

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

Configuration to disable BToE.

ID	FZI-2019-3
Manufacturer	Poly
Product	VVX 410, VVX 411
Affected Version	UC Software <= 6.1.0.6189
Patch	-
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

1.4 Unauthenticated Access to SIP Service

By default, the phone runs a SIP service, which can be abused to leak information, fake the caller identity and issue outgoing calls. This vulnerability has been reported earlier for the VVX 500 and VVX 601, however it hasn't been fixed for all affected phone models. Furthermore, the vulnerability cannot only be used to leak information but also to fake the caller identity and issue outgoing calls. The vulnerability can be mitigated by setting the following configuration option:

```
voIpProt.SIP.requestValidation.1.request="All"
```

Configuration to enable request validation.

ID	FZI-2019-4
Manufacturer	Poly
Product	VVX 410, VVX 411
Affected Version	UC Software <= 6.1.0.6189
Patch	-
CVSS Score	7.3
CVSS String	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

2 Disclosure Timeline

- 17.07.18: Initial notification to Poly
- 23.07.18 - 07.08.18: Reproduce vulnerability with Poly
- 07.08.18 – 19.10.18: No answer from Poly
- 19.10.18 - 07.12.18: Search for new contact person
- 11.12.18 – 16.07.19: Communication with new contact person
- 16.07.19: Disclosure with responsible disclosure policy
- 19.07.19: Workaround for SIP vulnerability
- 19.09.19: Patch for buffer overflow
- 15.10.19: Publication