Advisory ID:	Auerswald-1200IP-20190102-WebInterface
Last Updated:	2019 January 30
Published:	2019 February 4
Version:	1.0
CVSS-Score:	9.0
Severity:	high
CVE:	CVE-2018-19977 (Command injection in ftp upgrade configuration) CVE-2018-19978 (Buffer Overflow in DHCP und PPPOE configuration)

Summary

A vulnerability in the web interface of the affected products could allow an unauthenticated remote attacker to trigger several vulnerabilities in the webserver. The attacker has to be in the same network and authenticated as simple user to the phone’s web server.

CVE-2018-19977 (Command injection in ftp upgrade configuration):
An attacker could exploit this vulnerability using command injection in ftp upgrade configuration of an affected device. The vulnerability is due to lack of proper input validation.
The update feature is not available for a normal user in the web interface, only for admin user. But this policy is only enforced on the client side. An attacker which has user privileges, can also trigger this exploit.

There are no direct workarounds that address this vulnerability.

CVE-2018-19978 (Buffer Overflow in DHCP und PPPOE configuration)
If the attacker can control the Hostname or ManufacturerName input value of the DHCP configuration, he/she can overflow the &buffer. The input validation and length limitation for the input values are handled only on client side. Thus, a curl command can trigger the overflow.

A similar vulnerability is in the PPoE configuration.

A normal user can trigger the code execution and will get a root shell, which is equivalent to a user with higher privileges.

There are no direct workarounds that address this vulnerability.

Affected Products

Web-Interface of COMfortel 1200IP

Workaround

There are no direct workarounds that address these vulnerabilities but to restrict access of attackers as the listed vulnerabilities require an authenticated access to the WebUI of the telephone. To limit this access, common security methods for VoIP networks should be properly implemented:

a) Restrict remote access to the web-interface: Access to the WebUI of the telephone should be limited to a well-known group of people. This can be achieved by isolating the VoIP network using VLAN or physical separation from the general network in combination with a restrictive firewall.

b) Restrict users being allowed to access the web-interface: In a lot of application scenarios, it is not necessary for users to access the WebUI of the telephone. In these cases, the user password should be implemented, but not be distributed.
c) Ensure usage of good passwords: Both, the user and admin passwords should be complex enough and not guessable. Advisory may be found in CWE-521.

Source

Auerswald would like to thank security researcher Stephan Huber from Fraunhofer Institute for Secure Information Technology (SIT) for reporting these vulnerabilities.