

Advisory ID: Auerswald-COMfortel-Webinterface-20210910

Last Updated: 15 November 2021

Published: 15 November 2021

Version: 1.0

CVE-2021-40856 (Auerswald COMfortel Authentication Bypass)

Affected Products

COMfortel 1400 IP, COMfortel 2600 IP, COMfortel 3600 IP

Summary

Some vulnerability in the web interface of the affected products could allow an attacker to gain full access to the device without using the login credentials. If unallowed access has been detected, sensitive personal information may have been compromised and action according to data protection laws might be necessary.

CVE-2021-40856 (Auerswald COMfortel Authentication Bypass)

Severity: high

Some vulnerability in the web interface of the affected products could allow an attacker to gain access to the device without using the login credentials. The attacker must have access to the web interface. This method allows access to protected files containing sensitive information. The attacker could use the acquired data to login to the web interface of the telephone or the PBX system and make charged calls. If unallowed access has been detected, sensitive personal information may have been compromised and action according to data protection laws might be necessary.

Workarounds:

COMfortel 1400 IP, COMfortel 2600 IP, COMfortel 3600 IP: Update to a firmware \geq 2.8G

Source

Auerswald would like to RedTeam Pentesting GmbH for reporting these vulnerabilities.