Advisory ID: Auerswald-PBX-Systems-Webinterface-20210910
Last Updated: 12 November 2021
Published: 12 November 2021
Version: 1.0
CVE-2021-40857 (Auerswald PBX Privilege Escalation)
CVE-2021-40858 (Auerswald PBX Arbitrary File Disclosure)
CVE-2021-40859 (Auerswald PBX Multiple Backdoors)

# Affected Products

COMpact 3000 ISDN, COMpact 3000 analog, COMpact 3000 VoIP
CVE-2021-40859

COMpact  4000, COMpact 5000(R), COMpact 5200(R), COMpact 5500R
COMmander 6000(R)(RX)
(CVE-2021-40857, CVE-2021-40858, CVE-2021-40859)

COMpact 5010 VoIP, COMpact 5020 VoIP
COMmander Business(19"), COMmander Basic.2(19")
(CVE-2021-40857, CVE-2021-40858, CVE-2021-40859)

# Summary

Some vulnerability in the web interface of the affected products could allow an attacker to gain full admin rights. The attacker must have access to the web interface.
Unallowed access to the PBX can be traced in the system log. If unallowed access has been detected, sensitive personal information may have been compromised and action according to data protection laws might be necessary.

**CVE-2021-40857 (Auerswald PBX Privilege Escalation)**

Severity: high

Attackers who have acquired access to a user account can log into the web-based management interface of the affected systems and access clear text passwords for other user accounts, including those with the "sub-admin" privilege.

**CVE-2021-40858 (Auerswald PBX Arbitrary File Disclosure)**

Severity: medium

Attackers who already have acquired administrative access as a so-called "sub-admin" (see above) can access the password for the highly privileged "Admin" account. This account can use all functions of the PBX and is allowed to apply firmware updates.

**CVE-2021-40859 (Auerswald PBX Multiple Backdoors)**

Severity: high

Attackers who have access to the web interface of the PBX can easily discover two passwords used for special service accounts. Using these passwords, attackers are granted Admin access to the PBX. All information needed to derive the passwords can be requested over the web interface without authentication.

# Workarounds:

COMpact 3000 ISDN, COMpact 3000 analog, COMpact 3000 VoIP: Update to a firmware >= 4.0T

COMpact  4000, COMpact 5000(R), COMpact 5200(R), COMpact 5500R, COMmander 6000(R)(RX): Update to a firmware >= 8.2B

COMpact 5010 VoIP, COMpact 5020 VoIP, COMmander Business(19"), COMmander Basic.2(19"): There are no direct workarounds that address these vulnerabilities but to restrict access of attackers as the listed vulnerabilities require access to the WebUI of the PBX. 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 PBX 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 of the PBX: In a lot of application scenarios, it is not necessary for users to access the WebUI of the PBX at all. 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.

# Source

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