

SSA-552702: Privilege Escalation Vulnerability in the Web Interface of SCALANCE and RUGGEDCOM Products

Publication Date: 2022-10-11
 Last Update: 2022-10-11
 Current Version: V1.0
 CVSS v3.1 Base Score: 8.8

SUMMARY

The products listed below do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations

SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations

SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V7.1.2	Update to V7.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109813051/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (6GK5766-1GE00-7DA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (6GK5766-1GE00-7DB0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 6GHz (6GK5766-1JE00-7DA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE WAM766-1 EEC (6GK5766-1GE00-7TA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (6GK5766-1GE00-7TB0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC 6GHz (6GK5766-1JE00-7TA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (6GK5766-1GE00-3DA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (6GK5766-1GE00-3DB0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 6GHz (6GK5766-1JE00-3DA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (SC, PN) (6GK5205-3BB00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BB00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BD00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB205-3 (ST, PN) (6GK5205-3BD00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB205-3LD (SC, E/IP) (6GK5205-3BF00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XB205-3LD (SC, PN) (6GK5205-3BF00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB208 (E/IP) (6GK5208-0BA00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB208 (PN) (6GK5208-0BA00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (SC, E/IP) (6GK5213-3BD00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (SC, PN) (6GK5213-3BD00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (ST, E/IP) (6GK5213-3BB00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB213-3 (ST, PN) (6GK5213-3BB00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB213-3LD (SC, E/IP) (6GK5213-3BF00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB213-3LD (SC, PN) (6GK5213-3BF00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB216 (E/IP) (6GK5216-0BA00-2TB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XB216 (PN) (6GK5216-0BA00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2 (SC) (6GK5206-2BD00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2 (ST/BFOC) (6GK5206-2BB00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XC206-2G PoE (6GK5206-2RS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2G PoE (54 V DC) (6GK5206-2RS00-5AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2G PoE EEC (54 V DC) (6GK5206-2RS00-5FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP (6GK5206-2BS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP EEC (6GK5206-2BS00-2FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP G (6GK5206-2GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP G (EIP DEF.) (6GK5206-2GS00-2TC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC206-2SFP G EEC (6GK5206-2GS00-2FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC208 (6GK5208-0BA00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC208EEC (6GK5208-0BA00-2FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC208G (6GK5208-0GA00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC208G (EIP def.) (6GK5208-0GA00-2TC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC208G EEC (6GK5208-0GA00-2FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC208G PoE (6GK5208-0RA00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XC208G PoE (54 V DC) (6GK5208-0RA00-5AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216 (6GK5216-0BA00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216-3G PoE (6GK5216-3RS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216-3G PoE (54 V DC) (6GK5216-3RS00-5AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216-4C (6GK5216-4BS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216-4C G (6GK5216-4GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216-4C G (EIP Def.) (6GK5216-4GS00-2TC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216-4C G EEC (6GK5216-4GS00-2FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC216EEC (6GK5216-0BA00-2FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC224 (6GK5224-0BA00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC224-4C G (6GK5224-4GS00-2AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC224-4C G (EIP Def.) (6GK5224-4GS00-2TC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XC224-4C G EEC (6GK5224-4GS00-2FC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204 (6GK5204-0BA00-2GF2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XF204 DNA (6GK5204-0BA00-2YF2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA (6GK5204-2AA00-2GF2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XF204-2BA DNA (6GK5204-2AA00-2YF2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM408-4C (6GK5408-4GP00-2AM2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM408-8C (6GK5408-8GS00-2AM2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM416-4C (6GK5416-4GS00-2AM2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XP208 (6GK5208-0HA00-2AS6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XP208 (Ethernet/IP) (6GK5208-0HA00-2TS6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XP208EEC (6GK5208-0HA00-2ES6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XP208PoE EEC (6GK5208-0UA00-5ES6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XP216 (6GK5216-0HA00-2AS6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XP216 (Ethernet/IP) (6GK5216-0HA00-2TS6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XP216EEC (6GK5216-0HA00-2ES6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XP216POE EEC (6GK5216-0UA00-5ES6): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324WG (24 x FE, AC 230V) (6GK5324-0BA00-3AR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR324WG (24 X FE, DC 24V) (6GK5324-0BA00-2AR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR326-2C PoE WG (6GK5326-2QS00-3AR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR326-2C PoE WG (without UL) (6GK5326-2QS00-3RR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3AR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3RR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24XFE, 4XGE, 24V) (6GK5328-4FS00-2AR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (24xFE, 4xGE,DC24V) (6GK5328-4FS00-2RR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (28xGE, AC 230V) (6GK5328-4SS00-3AR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR328-4C WG (28xGE, DC 24V) (6GK5328-4SS00-2AR3): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (6GK5528-0AA00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (6GK5552-0AA00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE XC206-2 (6AG1206-2BB00-7AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE XC206-2SFP (6AG1206-2BS00-7AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE XC208 (6AG1208-0BA00-7AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE XC216-4C (6AG1216-4BS00-7AC2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Use ACLs to restrict access to the device web server
- Restrict access to the device web server ports (default 443/tcp or 80/tcp) to trusted networks and client IP addresses

Product-specific remediations or mitigations can be found in the section [Affected Products and Solution](#). Please follow the [General Security Recommendations](#).

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: <https://www.siemens.com/industrialsecurity>

PRODUCT DESCRIPTION

SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

SCALANCE W-1700 products are wireless communication devices based on IEEE 802.11ac standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

SCALANCE W-700 products are wireless communication devices based on IEEE 802.11ax or 802.11n standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (<https://www.first.org/cvss/>). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: <https://cwe.mitre.org/>.

Vulnerability CVE-2022-31765

Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-862: Missing Authorization

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Martin Grubhofer and Michael Messner from Siemens Energy for reporting the vulnerability

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

<https://www.siemens.com/cert/advisories>

HISTORY DATA

V1.0 (2022-10-11): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.