SSA-913875: Frame Aggregation and Fragmentation Vulnerabilities in 802.11

Publication Date: 2021-07-13
Last Update: 2025-04-08
Current Version: V1.4
CVSS v3.1 Base Score: 6.5

SUMMARY

Twelve vulnerabilities in the implementation of frame aggregation and fragmentation of the 802.11 standard, under the name of FragAttacks, have been published.

Successful exploitation of these vulnerabilities could allow an attacker within Wi-Fi range to forge encrypted frames, which could result in sensitive data disclosure and possibly traffic manipulation.

The advised Siemens products are only affected by some of the published vulnerabilities.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D family:	Update to V8.7.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109802805/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D (JP) (6GK5750-2HX01-1AD0): All versions < V8.7.1.3 affected by CVE-2020-24588, CVE-2020-26146	Update to V8.7.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109802805/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D (ROW) (6GK5750-2HX01-1AA0): All versions < V8.7.1.3 affected by CVE-2020-24588, CVE-2020-26146	Update to V8.7.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109802805/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D (USA) (6GK5750-2HX01-1AB0): All versions < V8.7.1.3 affected by CVE-2020-24588, CVE-2020-26146	Update to V8.7.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109802805/ See further recommendations from section Workarounds and Mitigations

SCALANCE W-700 IEEE 802.11ax family:	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (6GK5766-1GE00-7DA0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (6GK5766-1GE00-7TA0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations

SCALANCE WUM766-1 (6GK5766-1GE00-3DA0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (USA) (6GK5766-1GE00-3DB0): All versions < V1.2.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109805887/ See further recommendations from section Workarounds and Mitigations
SCALANCE W-700 IEEE 802.11n family:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0): All versions affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26143, CVE-2020-26144, CVE-2020-26146, CVE-2020-26147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W-1700 IEEE 802.11ac family:	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions < V3.0.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions < V3.0.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions < V3.0.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions < V3.0.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions < V3.0.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations

SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions < V3.0.0 affected by CVE-2020-24588, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further 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:

- CVE-2020-24588, CVE-2020-26144: Disable A-MSDU, if possible
- As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls

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 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 W1750D is an Access Point that supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with two dual-band radios, which can provide access and monitor the network simultaneously.

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.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2020-24588

The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.

CVSS v3.1 Base Score	3.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2020-26139

An issue was discovered in the kernel in NetBSD 7.1. An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2020-26140

An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Vulnerability CVE-2020-26141

An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The Wi-Fi implementation does not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-354: Improper Validation of Integrity Check Value

Vulnerability CVE-2020-26143

An issue was discovered in the ALFA Windows 10 driver 1030.36.604 for AWUS036ACH. The WEP, WPA, WPA2, and WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26144

An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid RFC1042 (i.e., LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26145

An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26146

An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WPA, WPA2, and WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-26147

An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:N
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

For more details regarding the FragAttacks vulnerabilities refer to:

- Fragment and Forge Breaking Wi-Fi Through Frame Aggregation and Fragmentation: https://papers.mathyvanhoef.com/usenix2021.pdf

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 (2021-07-13):	Publication Date
V1.1 (2021-10-12):	Added fix for SCALANCE W1750D
V1.2 (2022-02-08):	Added fix for SCALANCE W-700 IEEE 802.11ax family; updated name and split into individual products the SCALANCE W-700 and SCALANCE W-1700 families; clarified that no fix is planned for SCALANCE W-700 IEEE 802.11n and SCALANCE W-1700 IEEE 802.11ac families
V1.3 (2022-04-12):	Added fix for SCALANCE W-1700 IEEE 802.11ac family
V1.4 (2025-04-08):	Clarified fix version information for SCALANCE W-700 IEEE 802.11ax family

TERMS OF USE