Alcatel-Lucent Security Advisory No. SA-N0096 Ed. 01

OmniAccess Stellar 802.11 Frame Aggregation and Fragmentation Vulnerabilities

Summary

Multiple vulnerabilities related to different components in the implementation of the IEEE 802.11 standard have been published affecting Access Points or WiFi clients or both. Successful exploitation of these vulnerabilities can result in sensitive data exfiltration and possibly manipulation of network traffic.

The vulnerabilities are identified with the following CVE s

CVE-2020-24586, CVE-2020-24587, CVE-2020-24588, CVE-2020-26139, CVE-2020-26140, CVE-2020-26141, CVE-2020-26142, CVE-2020-26143, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146, CVE2020-26147

Description of the Vulnerability

Vulnerabilities in the implementation of the IEEE 802.11 standard have been reported in a paper by Mathy Vanhoef from New York University Abu Dhabi. These vulnerabilities, which have been collectively named FragAttacks, allow an attacker to inject malicious frames in legitimate WiFi connections, regardless of the type of wireless encryption used. Successful exploitation of these vulnerabilities could result in exfiltration of sensitive data or, when used in conjunction with other known attacks, could allow for the manipulation of network traffic. These vulnerabilities impact WiFi Access Points and/or WiFi clients. This vulnerability notice focuses on the impact to OmniAccess Stellar WLAN products. Please check with the supplier of client devices used in your network for details related to these products.

The two vulnerabilities affecting OmniAccess Stellar APs, CVE-2020-24588 and CVE-2020-26146, are described in more detail below.

Accepting non-SPP A-MSDU frames (CVE-2020-24588)

Severity: MEDIUM

CVSSv3 Overall Score: 6.1

When small packets are being sent it can be more efficient to aggregate multiple packets into a single frame for transmission on the wireless network. The IEEE 802.11 standard defines Aggregate MAC Service Data Units (A-MSDUs) to allow this aggregation. In an A-MSDU frame, the A-MSDU flag in the QoS field is Set indicating the payload field contains one or more subframes. By default, the A-MSDU flag is not authenticated unless the sender and receiver support Signaling and Payload Protected (SPP). As a result, devices that do not support SPP can be manipulated to process normal frames as A-MSDUs, and vice versa. By using a MitM (Machine-in-the-Middle) attack and altering the A-MSDU bit from the QoS filed in the MAC header, an attacker could access to sensitive data or inject data in frames sent to the target.

Reassembling encrypted fragments with non-consecutive packet numbers (CVE-2020-26146)

Severity: MEDIUM

CVSSv3 Overall Score: 4.7

The IEEE 802.11 standard allows for fragmentation of data frames that are larger than a particular value into more than one MAC Protocol Data Unit (MPDU) for transmission on the wireless network. On the receiving device, these fragments are then reassembled into the original data frame. The MAC header includes a Sequence Number (SN) subfield for ordering of the MPDUs and a Fragment Number (FN) subfield; fragments of one data frame have the same SN but different FN. Finally, once encrypted, the MPDUs also have a Packet Number (PN) which is a consecutively increasing number used to defend against replay attacks. PNs are expected to increase linearly with FNs and SNs. The OmniAccess Stellar Access Points do not validate that all fragments of a frame have consecutive PNs to confirm that the fragments belong to the same frame or not. An attacker using a MitM (Machine-in-the-Middle) attack could exploit this vulnerability by mixing fragments of different packets to extract user data.

Status on Alcatel-Lucent Enterprise Products

The OmniAccess Stellar products that are impacted by the vulnerabilities are identified below.

Product Name	Release
OmniAccess Stellar models impacted by CVE-2020-24588 – OAW-AP1101, OAW-AP12xx, OAW-AP13xx	AWOS 4.0.2 or earlier
OmniAccess Stellar models impacted by CVE-2020-26146 – OAW-AP1101, OAW-AP12xx	AWOS 4.0.2 or earlier

Workarounds

There are no workarounds for the specific vulnerabilities. The following best practices for a WLAN deployment can mitigate the impact of attacks.

- Enable Wireless Intrusion Protection System (WIPS) on the network. WIPS scans the wireless network to detect and mitigate MitM attacks on the network from rogue access points. WIPS also aids in detecting many other attacks that can be launched against wireless devices. Several of the OmniAccess Stellar APs have a dedicated scanning radio.
- Enable EAP-TLS which allows the network to authenticate the client and the client to authenticate the network. This mitigates the ability for rogue access points to establish connectivity to client devices on the network.
- Enable WPA3 which provides for 802.11w protected management frames, thereby preventing rogue devices from issuing deauthorization/disassociation frames and impacting the connection between AP and client. WPA3 reduces the likelihood of a successful MitM attack.

Resolution for Alcatel-Lucent Enterprise affected products

Information on software versions to address the vulnerabilities is provided below.

Product	Fixed in	Date
Omni Access Stellar - all models	AWOS 4.0.2 MR2	Targeted release is July 2021

History

Ed.01 (2021 May 26): creation