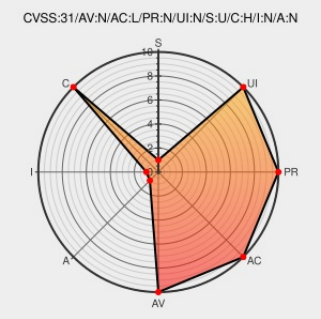
CVE-2020-12266

Published on: 04/27/2020 12:00:00 AM UTC

Last Modified on: 04/29/2022 01:25:00 PM UTC

CVE-2020-12266

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jetstream Ac3000 from Wavlink contain the following vulnerability:

An issue was discovered where there are multiple externally accessible pages that do not require any sort of authentication, and store system information for internal usage. The devices automatically query these pages to update dashboards and other statistics, but the pages can be accessed externally without any authentication. All the pages follow the naming convention live_(string).shtml. Among the information disclosed is: interface status logs, IP address of the device, MAC address of the device, model and current firmware version, location, all running processes, all interfaces and their statuses, all current DHCP leases and the associated hostnames, all other wireless networks in range of the router, memory statistics, and components of the configuration of the device such as enabled features. Affected devices: Affected devices are: Wavlink WN530HG4, Wavlink WN575A3, Wavlink WN579G3,Wavlink WN531G3, Wavlink WN533A8, Wavlink WN531A6, Wavlink WN551K1, Wavlink WN535G3, Wavlink WN530H4, Wavlink WN57X93, WN572HG3, Wavlink WN578A2, Wavlink WN579G3, Wavlink WN579X3, and Jetstream AC3000/ERAC3000

CVE-2020-12266 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
WAVLINK.COM UNDER CONSTRUCTION	Vendor Advisory www.wavlink.com text/html	MISC www.wavlink.com
GitHub - Roni-Carta/nyra	github.com text/html	MISC github.com/Roni-Carta/nyra
CVE/CVE-2020-12266-affected_devices at master · sudo-jtcsec/CVE · GitHub	github.com text/html	MISC github.com/sudo-jtcsec/CVE/blob/master/CVE-2020-12266-affected_devices
GitHub - sudo-jtcsec/Nyra: If you have a Wavlink router, its Not Your Router Anymore	github.com text/html	MISC github.com/sudo-jtcsec/Nyra
CVE/CVE-2020-12266 at master · sudo-jtcsec/CVE · GitHub	Third Party Advisory github.com text/html	MISC github.com/sudo-jtcsec/CVE/blob/master/CVE-2020-12266

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Wavlink	Jetstream Ac3000	-	All	All	All
Operating System	Wavlink	Jetstream Ac3000 Firmware	-	All	All	All
Hardware	Wavlink	Jetstream Erac3000	-	All	All	All
Operating System	Wavlink	Jetstream Erac3000 Firmware	-	All	All	All
Hardware	Wavlink	WI-wn530hg4	-	All	All	All
Hardware	Wavlink	WI-wn530hg4	-	All	All	All
Operating System	Wavlink	WI-wn530hg4 Firmware	m30hg4.v5030.191116	All	All	All
Operating System	Wavlink	WI-wn530hg4 Firmware	m30hg4.v5030.191116	All	All	All
Hardware	Wavlink	WI-wn575a3	-	All	All	All
Hardware	Wavlink	WI-wn575a3	-	All	All	All

Operating System	Wavlink	Wl-wn575a3 Firmware	rpt75a3.v4300.180801	All	All	All
Operating System	Wavlink	Wl-wn575a3 Firmware	rpt75a3.v4300.180801	All	All	All
Hardware	Wavlink	Wl-wn579g3	-	All	All	All
Hardware	Wavlink	Wl-wn579g3	-	All	All	All
Operating System	Wavlink	Wl-wn579g3 Firmware	m79x3.v5030.180719	All	All	All
Operating System	Wavlink	Wl-wn579g3 Firmware	m79x3.v5030.180719	All	All	All
Hardware	Wavlink	Wn530h4	-	All	All	All
Operating System	Wavlink	Wn530h4 Firmware	-	All	All	All
Hardware	Wavlink	Wn531a6	-	All	All	All
Operating System	Wavlink	Wn531a6 Firmware	-	All	All	All
Hardware	Wavlink	Wn531g3	-	All	All	All
Operating System	Wavlink	Wn531g3 Firmware	-	All	All	All
Hardware	Wavlink	Wn533a8	-	All	All	All
Operating System	Wavlink	Wn533a8 Firmware	-	All	All	All
Hardware	Wavlink	Wn535g3	-	All	All	All
Operating System	Wavlink	Wn535g3 Firmware	-	All	All	All
Hardware	Wavlink	Wn551k1	-	All	All	All
Operating System	Wavlink	Wn551k1 Firmware	-	All	All	All
Hardware	Wavlink	Wn578a2	-	All	All	All
Operating System	Wavlink	Wn578a2 Firmware	-	All	All	All
Hardware	Wavlink	Wn579g3	-	All	All	All
Operating System	Wavlink	Wn579g3 Firmware	-	All	All	All
Hardware	Wavlink	Wn579x3	-	All	All	All
Operating System	Wavlink	Wn579x3 Firmware	-	All	All	All
Hardware	Wavlink	Wn57x93	-	All	All	All
Operating System	Wavlink	Wn57x93 Firmware	-	All	All	All

cpe:2.3:h:wavlink:jetstream_ac3000:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:jetstream_ac3000_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:jetstream_erac3000:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:jetstream_erac3000_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wl-wn530hg4:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wl-wn530hg4:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wl-wn530hg4_firmware:m30hg4.v5030.191116:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wl-wn530hg4_firmware:m30hg4.v5030.191116:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wl-wn575a3:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wl-wn575a3:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wl-wn575a3_firmware:rpt75a3.v4300.180801:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wl-wn575a3_firmware:rpt75a3.v4300.180801:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wl-wn579g3:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wl-wn579g3:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wl-wn579g3_firmware:m79x3.v5030.180719:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wl-wn579g3_firmware:m79x3.v5030.180719:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn530h4:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn530h4_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn531a6:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn531a6_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn531g3:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn531g3_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn533a8:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn533a8_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn535g3:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn535g3_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn551k1:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn551k1_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn578a2:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn578a2_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn579g3:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn579g3_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn579x3:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn579x3_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:wavlink:wn57x93:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn57x93_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | An issue was discovered where there are ... | CVE-2020-12266 | Link for more: alerts.remotelyrmm.com/CVE-2020-12266	2022-04-29 14:35:21

← Previous ID

Next ID→