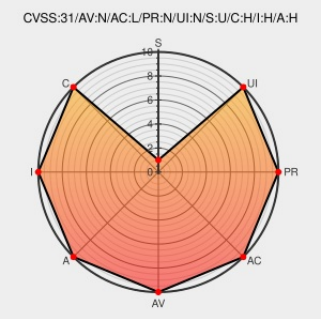
CVE-2019-15310

Published on: 07/01/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-15310

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



Certain versions of Linkplay from Linkplay contain the following vulnerability:

An issue was discovered on various devices via the Linkplay firmware. There is WAN remote code execution without user interaction. An attacker could retrieve the AWS key from the firmware and obtain full control over Linkplay's AWS estate, including S3 buckets containing device firmware. When combined with an OS command injection vulnerability within the XML Parsing logic of the firmware update process, an attacker would be able to gain code execution on any device that attempted to update. Note that by default all devices tested had automatic updates enabled.

CVE-2019-15310 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

Linkplay Firmware WAN/LAN Remote Code Execution	Exploit Third Party Advisory labs.f-secure.com text/html	MISC labs.f-secure.com/advisories/linkplay-firmware-wanlan-remote-code-execution/
LinkPlay - Wireless audio devices from USA, Europe, Asia	Product web.archive.org text/html Inactive Link Not Archived	MISC linkplay.com/featured-products/
Advisories - MWR Labs	Third Party Advisory labs.mwrinfosecurity.com text/html	MISC labs.mwrinfosecurity.com/advisories/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linkplay	Linkplay	-	All	All	All
Operating System	Linkplay	Linkplay	-	All	All	All

cpe:2.3:o:linkplay:linkplay:-:*:*:*:*:*:*:*:

cpe:2.3:o:linkplay:linkplay:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→