



# CVE-2018-20575

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-20575
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-28 17:29:00 UTC
<b>Updated</b>	2019-01-23 21:15:00 UTC
<b>Description</b>	Orange Livebox 00.96.320S devices have an undocumented /system_firmware.stm URI for manual firmware update. This i

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Orange	Arv7519rw22 Livebox 2.1	-	All	All	All
Hardware	Orange	Arv7519rw22 Livebox 2.1	-	All	All	All
Operating System	Orange	Arv7519rw22 Livebox 2.1 Firmware	00.96.320s	All	All	All
Operating System	Orange	Arv7519rw22 Livebox 2.1 Firmware	00.96.320s	All	All	All

## References

### Reference

- GitHub - zadewg/LIVEBOX-0DAY: Arcadyan ARV7519RW22-A-L T VR9 1.2 Multiple security vulnerabilities affecting latest firmware release o
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)