



# CVE-2020-27488

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2020-27488                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | cve@mitre.org                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2021-01-13 20:15:00 UTC                                                                                                    |
| <b>Updated</b>         | 2021-01-21 16:58:00 UTC                                                                                                    |
| <b>Description</b>     | Loxone Miniserver devices with firmware before 11.1 (aka 11.1.9.3) are unable to use an authentication method that is base |

## Risk And Classification

### Problem Types: CWE-287

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                                   | Version | Update | Edition | Language |
|------------------|------------------------|-------------------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Loxone</a> | <a href="#">Miniserver Gen 1</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Loxone</a> | <a href="#">Miniserver Gen 1</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Loxone</a> | <a href="#">Miniserver Gen 1 Firmware</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Loxone</a> | <a href="#">Miniserver Gen 1 Firmware</a> | All     | All    | All     | All      |

## References

| Reference                                                   | Source  | Link                                                                     | Tags                          |
|-------------------------------------------------------------|---------|--------------------------------------------------------------------------|-------------------------------|
| Advisory - Schwachstelle im Loxone Cloud DNS                | MISC    | <a href="https://github.com/iot-lab-fh-ooe">iot-lab-fh-ooe.github.io</a> | Exploit, Third Party Advisory |
| Advisory - Loxone Cloud DNS Vulnerability                   | MISC    | <a href="https://github.com/iot-lab-fh-ooe">iot-lab-fh-ooe.github.io</a> | Exploit, Third Party Advisory |
| Security Improvements for Loxone Cloud DNS - Loxone Blog    | MISC    | <a href="https://www.loxone.com">www.loxone.com</a>                      | Vendor Advisory               |
| Sicherheitsverbesserungen am Loxone Cloud DNS - Loxone Blog | MISC    | <a href="https://www.loxone.com">www.loxone.com</a>                      | Product, Vendor Advisory      |
| CVE Program record                                          | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                            | canonical                     |
| NVD vulnerability detail                                    | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                          | canonical, analysis           |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)