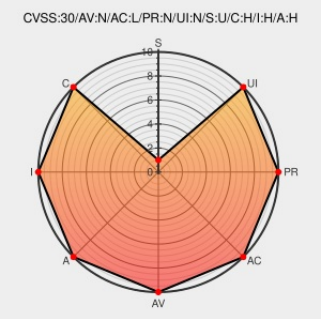
# CVE-2020-27868

Published on: 02/11/2021 12:00:00 AM UTC

Last Modified on: 03/26/2021 07:41:00 PM UTC

## CVE-2020-27868

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




Certain versions of Ocularis from Qognify contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Qognify Ocularis 5.9.0.395. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of serialized objects provided to the EventCoordinator endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-11257.

CVE-2020-27868 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Qognify** - **Ocularis** version **5.9.0.395**

### 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 |
| --- | --- | --- |
| ZDI-20-1453 \| Zero Day Initiative | Third Party Advisory<br>VDB Entry<br>www.zerodayinitiative.com<br>text/html | MISC www.zerodayinitiative.com/advisories/ZDI-20-1453/ |
| Software Downloads \| Qognify: Safeguarding Your World | www.qognify.com<br>text/html | MISC www.qognify.com/support-training/software-downloads/ |

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 |
| --- | --- | --- | --- | --- | --- | --- |
| Application | Qognify | Ocularis | 5.9.0.395 | All | All | All |
| Application | Qognify | Ocularis | 5.9.0.395 | All | All | All |

cpe:2.3:a:qognify:ocularis:5.9.0.395:*:*:*:*:*:*:*:

cpe:2.3:a:qognify:ocularis:5.9.0.395:*:*:*:*:*:*:*:

## Discovery Credit

Joachim Kerschbaumer (@joachimk)

← Previous ID

Next ID→