



# Miniorange OTP Verification with Firebase <= 3.6.0 - Privilege Escalation via Registration due to Administrator Default User Role Value

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

## Summary

<b>CVE</b>	CVE-2024-9863
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-10-17 02:15:04 UTC
<b>Updated</b>	2026-04-08 19:22:43 UTC
<b>Description</b>	The Miniorange OTP Verification with Firebase plugin for WordPress is vulnerable to privilege escalation in versions up to, ,

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from security@wordfence.com

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.006770000 probability, percentile 0.714950000 (date 2026-04-13)

**Problem Types:** CWE-266 | CWE-266 CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cyberlord92	Miniorange OTP Verification With Firebase	affected 3.6.0 semver	Not specified
ADP	Miniorange	Otp Verification	affected 3.6.0 semver	Not specified

### References

Reference	Source	Link
plugins.trac.wordpress.org/browser/miniorange-firebase-sms-otp-verification/tags/3.6.0/h...	security@wordfence.com	plugins.trac.wordpre
plugins.trac.wordpress.org/changeset/3169869/miniorange-firebase-sms-otp-verification	security@wordfence.com	plugins.trac.wordpre
www.wordfence.com/threat-intel/vulnerabilities/id/f04eab14-dd86-4145-b5eb-20d06...	security@wordfence.com	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

### Vendor Comments And Credit

Discovery Credit

**CNA:** István Márton (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-10-11T00:00:00.000Z	Discovered
CNA	2024-10-11T00:00:00.000Z	Vendor Notified
CNA	2024-10-16T00:00:00.000Z	Disclosed

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)