Orion SMS OTP Verification <= 1.1.7 - Authentication Bypass via Account Takeover

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-9967
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-15 09:15:43 UTC
Updated	2026-04-08 19:24:50 UTC
Description	The Orion SMS OTP Verification plugin for WordPress is vulnerable to privilege escalation via account takeover in all versic

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: 0.001740000 probability, percentile 0.387890000 (date 2026-04-13)

Problem Types: CWE-288 | CWE-288 CWE-288 Authentication Bypass Using an Alternate Path or Channel

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

ntegrity

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	Gsayed786	Orion SMS OTP Verification.	affected 1.1.7 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/log/orion-sms-otp-verification	security@wordfence.com	plugins.trac.wordpres
www.wordfence.com/threat-intel/vulnerabilities/id/b121fdb4-93a8-400c-89c2-3195c...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/orion-sms-otp-verification/trunk/vendor/js/reset-pass...	security@wordfence.com	plugins.trac.wordpres
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Jonas Benjamin Friedli (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-10-14T20:00:13.000Z	Disclosed

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