# CVE-2020-8644

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-8644 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-02-05 22:15:00 UTC |
| **Updated** | 2022-07-12 17:42:00 UTC |
| **Description** | PlaySMS before 1.4.3 does not sanitize inputs from a malicious string. |

## Risk And Classification

**EPSS:** 0.940620000 probability, percentile 0.999060000 (date 2026-05-18)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** CWE-94

## CISA Known Exploited Vulnerability

| | |
|---|---|
| **Vendor** | PlaySMS |
| **Product** | PlaySMS |
| **Name** | PlaySMS Server-Side Template Injection Vulnerability |
| **Required Action** | Apply updates per vendor instructions. |
| **Notes** | https://nvd.nist.gov/vuln/detail/CVE-2020-8644 |

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Playsms | Playsms | All | All | All | All |
| Application | Playsms | Playsms | All | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| PlaySMS index.php Unauthenticated Template Injection Code Execution ≈ Packet Storm | MISC | packets |
| playSMS 1.4.3 has been released | MISC | playsms |
| playSMS 1.4.3 has been released - News - playSMS Forum | MISC | forum.p |
| Technical Advisory – playSMS Pre-Authentication Remote Code Execution (CVE-2020-8644) – NCC Group Research | MISC | research |

| | | |
|---|---|---|
| Technical Advisory – playSMS Pre-Authentication Remote Code Execution (CVE-2020-8644) – NCC Group Research | MISC | researc |
| CVE Program record | CVE.ORG | www.cv |
| NVD vulnerability detail | NVD | nvd.nist |
| CISA Known Exploited Vulnerabilities catalog | CISA | www.cis |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

376481 PlaySMS Unauthenticated Template Injection Code Execution Vulnerability