# Unauthenticated Remote Code Execution (RCE) in SOY CMS

Critical **inunosinsi** published **GHSA-hrrx-m22r-p9jp** on Sep 16, 2020

Package

**SOY CMS**

| Affected versions | Patched versions |
| --- | --- |
| < 3.0.2.328 | 3.0.2.328 |

## Description

SOY CMS 3.0.2.327 and earlier is affected by Unauthenticated Remote Code Execution (RCE). The allows remote attackers to execute any arbitrary code when the inquiry form feature is enabled by the service. The vulnerability is caused by unserializing the form without any restrictions. This was fixed in 3.0.2.328.

Impact: Unauthenticated remote Code Execution via inquiry Form
・Attack vector is: Inquiry Form
・Tested SOY CMS Version: 3.0.2(latest)
・Affected SOY CMS Version: ～3.0.2
Found by **@stypr** from Vulnerability Research Team in Flatt Security Inc.

Additional Note:
It is different from CVE-2020-15182 and CVE-2020-15183 as (1) it does not require any permissions to achieve the attack (2) components are different (3) This vulnerability does not need any authentication to achieve the attack.

Reference:
Issue: #10
PR: #12
Exploit Video: https://youtu.be/zAE4Swjc-GU

### Severity

Critical

### CVE ID

CVE-2020-15188

### Weaknesses

No CWEs

### Credits

stypr