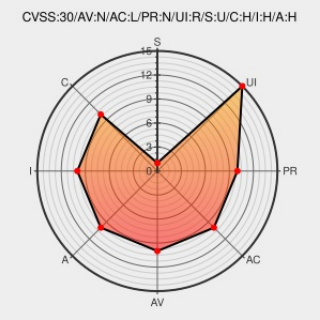
# CVE-2018-14057

Published on: 08/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

## CVE-2018-14057

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




Certain versions of Pimcore from Pimcore contain the following vulnerability:

Pimcore before 5.3.0 allows remote attackers to conduct cross-site request forgery (CSRF) attacks by leveraging validation of the X-pimcore-csrf-token anti-CSRF token only in the "Settings > Users / Roles" function.

CVE-2018-14057 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 8.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 6.8 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Pimcore 5.2.3 CSRF / Cross Site Scripting / SQL Injection ≈ Packet Storm | Exploit<br>Third Party Advisory<br>VDB Entry<br>packetstormsecurity.com | MISC<br>packetstormsecurity.com/files/148954/Pimcore-5.2.3-CSRF-Cross-Site-Scripting-SQL-Injection.html |

| | | |
|---|---|---|
| | text/html | |
| Pimcore 5.2.3 - SQL Injection / Cross-Site Scripting / Cross-Site Request Forgery - PHP webapps Exploit | Exploit<br>Third Party Advisory<br>VDB Entry<br>www.exploit-db.com<br>Proof of Concept<br>text/html | EXPLOIT-DB 45208 |
| SQL Injection, XSS & CSRF vulnerabilities in Pimcore software – SEC Consult | Exploit<br>Third Party Advisory<br>www.sec-consult.com<br>text/html | MISC www.sec-consult.com/en/blog/advisories/sql-injection-xss-csrf-vulnerabilities-in-pimcore-software/ |
| Full Disclosure: SEC Consult SA-20180813-0 :: SQL Injection, XSS & CSRF vulnerabilities in Pimcore | Exploit<br>Mailing List<br>Third Party Advisory<br>seclists.org<br>text/html | FULLDISC 20180816 SEC Consult SA-20180813-0 :: SQL Injection, XSS & CSRF vulnerabilities in Pimcore |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:pimcore:pimcore:*:*:*:*:*:*:*:*:

cpe:2.3:a:pimcore:pimcore:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→