# CVE Detail – CVE-2009-3759

Multiple cross-site request forgery (CSRF) vulnerabilities in sample code in the XenServer Resource Kit in Citrix XenCenterWeb allow remote attackers to hijack the authentication of administrators for (1) requests that change the password via the username parameter to config/changepw.php or (2) stop a virtual machine via the stop\_vmname parameter to hardstopvm.php. NOTE: some of these details are obtained from third party information.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.79414

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-352: Cross-Site Request Forgery (CSRF)

## CAPEC(s)

* CAPEC-111: JSON Hijacking (aka JavaScript Hijacking)
* CAPEC-462: Cross-Domain Search Timing
* CAPEC-467: Cross Site Identification
* CAPEC-62: Cross Site Request Forgery

## Affected Products

* cpe:2.3:a:citrix:xencenterweb:-:\*:\*:\*:\*:\*:\*:\*