



CVE-2013-4963

Published on: 03/14/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:28 PM UTC

CVE-2013-4963

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Puppet Enterprise](#) from [Puppet](#) contain the following vulnerability:

Multiple cross-site request forgery (CSRF) vulnerabilities in Puppet Enterprise (PE) before 3.0.1 allow remote attackers to hijack the authentication of users for requests that deleting a (1) report, (2) group, or (3) class or possibly have other unspecified impact.

CVE-2013-4963 has been assigned by [M](#) cve@mitre.org to track the vulnerability

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

CVE-2013-4963 | Puppet Labs

[Vendor Advisory](#)
[puppetlabs.com](#)
[text/html](#)

[CONFIRM puppetlabs.com/security/cve/cve-2013-4963](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Puppet	Puppet Enterprise	1.0	All	All	All
Application	Puppet	Puppet Enterprise	1.1	All	All	All
Application	Puppet	Puppet Enterprise	1.2.0	All	All	All
Application	Puppet	Puppet Enterprise	2.0.0	All	All	All
Application	Puppet	Puppet Enterprise	2.0.1	All	All	All
Application	Puppet	Puppet Enterprise	2.0.2	All	All	All
Application	Puppet	Puppet Enterprise	2.0.3	All	All	All
Application	Puppet	Puppet Enterprise	2.5.1	All	All	All
Application	Puppet	Puppet Enterprise	2.5.2	All	All	All
Application	Puppet	Puppet Enterprise	2.8.0	All	All	All
Application	Puppet	Puppet Enterprise	2.8.1	All	All	All
Application	Puppet	Puppet Enterprise	2.8.2	All	All	All
Application	Puppet	Puppet Enterprise	2.8.3	All	All	All
Application	Puppet	Puppet Enterprise	1.0	All	All	All
Application	Puppet	Puppet Enterprise	1.1	All	All	All
Application	Puppet	Puppet Enterprise	1.2.0	All	All	All
Application	Puppet	Puppet Enterprise	2.0.0	All	All	All
Application	Puppet	Puppet Enterprise	2.0.1	All	All	All
Application	Puppet	Puppet Enterprise	2.0.2	All	All	All
Application	Puppet	Puppet Enterprise	2.0.3	All	All	All
Application	Puppet	Puppet Enterprise	2.5.1	All	All	All
Application	Puppet	Puppet Enterprise	2.5.2	All	All	All
Application	Puppet	Puppet Enterprise	2.8.0	All	All	All
Application	Puppet	Puppet Enterprise	2.8.1	All	All	All
Application	Puppet	Puppet Enterprise	2.8.2	All	All	All
Application	Puppet	Puppet Enterprise	2.8.3	All	All	All
Application	Puppet	Puppet Enterprise	All	All	All	All
cpe:2.3:a:puppet:puppet_enterprise:1.0:*:*:*:*:*.*						
cpe:2.3:a:puppet:puppet_enterprise:1.1:*:*:*:*:*.*						
cpe:2.3:a:puppet:puppet_enterprise:1.2.0:*:*:*:*:*.*						
cpe:2.3:a:puppet:puppet_enterprise:2.0.0:*:*:*:*:*.*						
cpe:2.3:a:puppet:puppet_enterprise:2.0.1:*:*:*:*:*.*						
cpe:2.3:a:puppet:puppet_enterprise:2.0.2:*:*:*:*:*.*						

```
cpe:2.3:a:puppet:puppet_enterprise:2.0.3:*:*:*:*:*:*
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.5.1:::*:*:*.*.*.*.*
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.5.2:*:*:*:*:*:*
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:1.0:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:1.1:*:*:*:*:*:*
```

```
cpe:2.3:a:puppet:puppet_enterprise:1.2.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.0.1:::*:*:*:*.*
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.5.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.5.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.1:*:*:*:*:*.*
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:puppet:puppet_enterprise:2.8.3:*:*:*:*:*:*
```

```
cpe:2.3:a:puppet:puppet_enterprise:*:*:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report