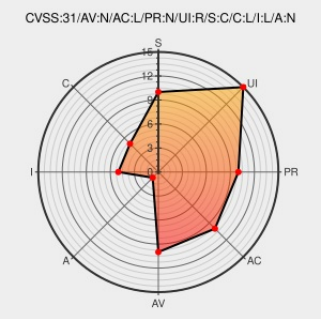
CVE-2015-5215

Published on: 02/17/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 08:08:49 PM UTC

CVE-2015-5215

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



Certain versions of Ipsilon from Ipsilon-project contain the following vulnerability:

** DISPUTED ** The default configuration of the Jinja templating engine used in the Identity Provider (IdP) server in Ipsilon 0.1.0 before 1.0.1 does not enable auto-escaping, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via template variables. NOTE: This may be a duplicate of CVE-2015-5216. Moreover, the Jinja development team does not enable auto-escape by default for performance issues as explained in https://jinja.palletsprojects.com/en/master/faq/#why-is-autoescaping-not-the-default.

CVE-2015-5215 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link

1255168 – (CVE-2015-5215) CVE-2015-5215 ipsilon: XSS in multiple pages	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1255168
Commit - ipsilon - a503aa9c2a30a74e709d1c88099befd50fb2eb16 - Pagure.io	Patch pagure.io text/html	MISC pagure.io/ipsilon/a503aa9c2a30a74e709d1c88099befd50fb2eb16
Releases/v1.0.1 – ipsilon	Product fedorahosted.org text/html	MISC fedorahosted.org/ipsilon/wiki/Releases/v1.0.1
oss-security - [CVE-2015-5215] Ipsilon: XSS in multiple pages	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2015/10/23/10

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ipsilon-project	Ipsilon	All	All	All	All
Application	Ipsilon-project	Ipsilon	All	All	All	All

cpe:2.3:a:ipsilon-project:ipsilon:*:*:*:*:*:*:*:*:

cpe:2.3:a:ipsilon-project:ipsilon:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→