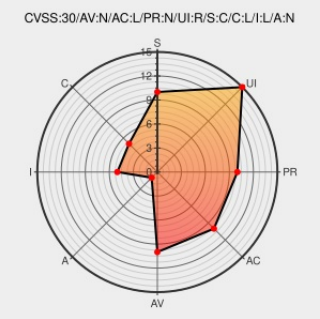
CVE-2015-3898

Published on: 02/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:08 PM UTC

CVE-2015-3898

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



Certain versions of Bonita Bpm Portal from Bonitasoft contain the following vulnerability:

Multiple open redirect vulnerabilities in Bonita BPM Portal before 6.5.3 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via vectors involving the redirectUrl parameter to (1) bonita/login.jsp or (2) bonita/loginservice.

CVE-2015-3898 has been assigned by cve@mitre.org 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: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
SecurityFocus	Exploit, Third Party Advisory, VDB Entry, www.securityfocus.com, text/html	BUGTRAQ 20150610 Arbitrary File Disclosure and Open Redirect in Bonita BPM

File Not Found	Exploit Third Party Advisory www.htbridge.com text/html Inactive Link Not Archived	MISC www.htbridge.com/advisory/HTB23259
Bonita BPM 6.5.1 Directory Traversal / Open Redirect ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/132237/Bonita-BPM-6.5.1-Directory-Traversal-Open-Redirect.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bonitasoft	Bonita Bpm Portal	All	All	All	All
Application	Bonitasoft	Bonita Bpm Portal	All	All	All	All

cpe:2.3:a:bonitasoft:bonita_bpm_portal:*:*:*:*:*:*:*:*:

cpe:2.3:a:bonitasoft:bonita_bpm_portal:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→