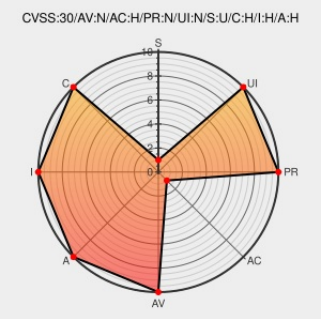
CVE-2015-5246

Published on: 10/06/2017 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:12:04 PM UTC

CVE-2015-5246

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



Certain versions of Foreman from Theforeman contain the following vulnerability:

The LDAP Authentication functionality in Foreman might allow remote attackers with knowledge of old passwords to gain access via vectors involving the password lifetime period in Active Directory.

CVE-2015-5246 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
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
Bug #11471: CVE-2015-5246 - previous password still allowed to log into foreman with Active Directory backend - Foreman	Issue Tracking Patch Vendor Advisory projects.theforeman.org text/html	CONFIRM projects.theforeman.org/issues/11471

1258700 – (CVE-2015-5246) CVE-2015-5246 Foreman: previous password still allowed to log into foreman with Active Directory backend	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1258700

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Theforeman	Foreman	1.9.0	All	All	All
Application	Theforeman	Foreman	1.9.0	All	All	All

cpe:2.3:a:theforeman:foreman:1.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→