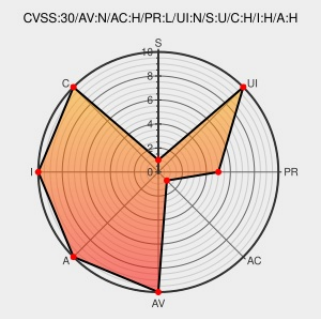
CVE-2018-1000133

Published on: 03/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1000133

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



Certain versions of Trident from Secluded contain the following vulnerability:

Pitchfork version 1.4.6 RC1 contains an Improper Privilege Management vulnerability in Trident Pitchfork components that can result in A standard unprivileged user could gain system administrator permissions within the web portal.. This attack appear to be exploitable via The user must be able to login, and could edit their profile and set the "System Administrator" permission to "yes" on themselves.. This vulnerability appears to have been fixed in 1.4.6 RC2.

CVE-2018-1000133 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
'Trident' Trusted	Third Party Advisory	MISC:themes.ward.net/security-advisories/trident-trusted-communications

Trident Trusted Communications Platform: Privilege Escalation Issue Advisory – Thomas Ward's Site	Third Party Advisory thomas-ward.net text/html	MISC thomas-ward.net/security-advisories/trident-trusted-communications-platform-privilege-escalation-issue-advisory/
Fixing issue that Thomas pointed out · tridentli/pitchfork@33549f1 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/tridentli/pitchfork/commit/33549f15707801099e1253dd5e79369bd48eb59b
Fixing issue that Thomas pointed out · tridentli/pitchfork@9fd07cb · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/tridentli/pitchfork/commit/9fd07cbe4f93e1367e142016e9a205366680dd54
Release 1.4.6-Release Candidate 2 · tridentli/trident · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/tridentli/trident/releases/tag/DEV_1.4.6-RC2
Resolve Perms isssue for Thomas · Issue #168 · tridentli/pitchfork · GitHub	Issue Tracking Third Party Advisory github.com text/html	CONFIRM github.com/tridentli/pitchfork/issues/168

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Secluded	Trident	1.4.6	rc1	All	All
Application	Secluded	Trident	1.4.6	rc1	All	All

cpe:2.3:a:secluded:trident:1.4.6:rc1:*:*:*:*:*:*:

cpe:2.3:a:secluded:trident:1.4.6:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→