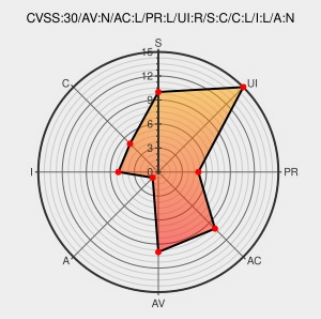
CVE-2017-14922

Published on: 09/29/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14922

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



Certain versions of Tine 2.0 from Tine20 contain the following vulnerability:

Stored XSS vulnerability via IMG element at "History" of Profile, Calendar, Tasks, and CRM in Tine 2.0 Community Edition before 2017.08.4 allows an authenticated user to inject JavaScript, which is mishandled during rendering by the application administrator and other users.

CVE-2017-14922 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
Releases · tine20/Tine-2.0-Open-Source-Groupware-and-CRM · GitHub	Issue Tracking, Patch, Release Notes	MISC github.com/tine20/Tine-2.0-Open-Source-Groupware-and-CRM/releases

	Third Party Advisory github.com text/html	
node exists exception broken · tine20/tine20@24e39e1 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/tine20/Tine-2.0-Open-Source-Groupware-and-CRM/commit/24e39e1e930097b8793a03b8864d3c484ede546b
node delte might fail · tine20/tine20@146c5aa · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/tine20/Tine-2.0-Open-Source-Groupware-and-CRM/commit/146c5aaafd826c1c8990333c393bff6f64c90786
name might not be displayed correctly · tine20/tine20@bc8a6fb · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/tine20/Tine-2.0-Open-Source-Groupware-and-CRM/commit/bc8a6fbd3128cf5ef27d808f6c6ba869fdc2262b
oss-security - Stored XSS vulnerability in Tine 2.0 Community Edition <= 2017.08.3	Mailing List Patch Third Party Advisory openwall.com text/html	MISC openwall.com/lists/oss-security/2017/09/28/11

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tine20	Tine 2.0	All	All	All	All

cpe:2.3:a:tine20:tine_2.0:*:*:*:*:community:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→