ESUP-2009-AVI-001 - esup-helpdesk vulnerability

Usage and diffusion of this document

The security advices of the ESUP-Portail consortium concern softwares distributed by the consortium. It is the responsability of each recipient of this document not to diffuse it to other people for obvious security reasons.

Object	esup-helpdesk vulnerabiliy
Reference	ESUP-2009-AVI-001
First version	2009 January 12th
Latest version	2009 January 14th
Source	University of Rennes 1
Diffusion	Public
History	• 2009 January 12th: reception of the vulnerability • 2009 January 13th: validation of the vulnerability (Pascal Aubry) • 2009 January 14th: diffusion of release 3.16.0 (Pascal Aubry)
Attached files	none.

Risks

Identity theft by stealing session identifiers thanks to XSS attacks.

Affected systems

- esup-helpdesk distributions from 3.0.0 to 3.15.2

Summary

esup-helpdesk uses FCK Editor to enter ticket actions and edit FAQs. The HTML code entered this way is shown to the user as-is in the history of tickets and FAQs.

Description

- From 3.0.0 to 3.15.2, by loading a page that uses FCK Editor and disabling Javascript, it is possible to enter malicious code into the database, for instance by using HTML tags <script> or <iframe>. Afterthat the code is excuted by the users that view the affected ticket or FAQs.
- From 3.14.5 to 3.15.2, consequence of a mistake in the upgrade of FCK Editor (from 1.7.26 to 1.8), it is possible to enter arbitrary code without invalidating Javascript.

Javascript attacks include the steal of session identifiers, thus authorizating identity theft.

Solution

Release 3.16.0:

- removes the malicious tags entered by users before storing data to the database;
- removes the malicious code that could have been entered with previous releases.

Event if it is possible to trace the attacks (all the actions are traced in the application), it is strongly recommended to upgrade to release 3.16.0 or later as soon as possible.

Links

- Download esup-helpdesk: http://helpdesk.esup-portail.org
- ChangeLog