ESUP-2009-AVI-003 - 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-003
First version	2009 March 11th
Latest version	2009 March 11th
Source	The Apache Software Foundation
Diffusion	Public
History	• 2009 March 9th: discovery of the vulnerability • 2009 March 11th: diffusion of release 3.20.0 (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 3.19.6

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

esup-helpdesk uses the Apache MyFaces extensions provided by the Tomahawk library.

Version 1.1.5 of this library, used by all the esup-helpdesk v3 distributions, has an important security hole that allows the injection of arbitrary Javascript code.

Cross Site Scripting attacks include the steal of session identifiers, thus authorizating identity theft, they are detailed on the web site of iDefense Labs.

Solution

esup-helpdesk 3.20.0 embeds version Tomahawk 1.1.6, which fixes the vulnerability (see TOMAHAWK-983).

Upgrading to esup-helpdesk 3.20.0 or later as soon as possible is strongly recommended.

Links

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