Sakai Security Policy

version 3.1, 2009-04-07

NOTICE

If you uncover a security vulnerability in Sakai software please do not voice your concerns on any public listserv, blog or other open communication channel but instead notify the Sakai Foundation immediately at security@sakaifoundation.org. Please provide a callback telephone number so that we can contact you by telephone if it is deemed necessary.

INTRODUCTION

Sakai is an open-source software initiative that promotes knowledge sharing and information transparency. However, when dealing with security vulnerabilities the integrity of existing Sakai installations can be compromised by the premature public disclosure of security threats before the Sakai Community has had time to analyze, develop and distribute countermeasures through private channels to institutions and organizations that have implemented Sakai software. Recognizing this danger, the Sakai Foundation has developed a security policy that seeks to safeguard the security of existing Sakai installations as well as provide full public disclosure of Sakai security vulnerabilities in a timely manner.

REPORTING SECURITY ISSUES

Security vulnerabilities in Sakai should be reported immediately to the Sakai Foundation at security@sakaifoundation.org. When contacting the Foundation, please provide a callback telephone number so that we can contact you by phone if it is deemed necessary. Sakai Foundation staff and community developers, working with the original reporter of the vulnerability, will investigate the issue, determine versions affected, and, if necessary, develop and distribute as quickly as is possible a security update for the Sakai Community and general public.

GENERAL POLICIES

Issues identified as security-related are prioritized and addressed differently than functionality or other issues classified as bugs. Access to issues flagged as security vulnerabilities in Sakai's JIRA issue tracking system will be restricted to Sakai security contacts and members of the Sakai Security Work Group (see below). Discussion, analysis, code development and testing relevant to reported security vulnerabilities will be treated as confidential information.

The Sakai Foundation will work with Sakai Community members to develop fixes for both vulnerable released versions and vulnerable branches (up to a particular date or release number). Code commits for security-related fixes will seek to mask the nature of the vulnerability. This usually takes one of two forms: (1) the commit is held until a patch can be tested, distributed and implemented in known sites or (2) in the case of a fix to a less significant threat the commit may be checked in with limited commentary.

During our QA and release cycles security-related issues will receive priority. At a minimum, the Sakai Security WG will review outstanding security issues before the start of each QA cycle.

The Sakai Foundation will issue security advisories and security updates to the general public once existing Sakai installations have been notified and given time to patch their systems.

SECURITY WORK GROUP

The Sakai Community has instituted a Security Work Group (WG) composed of senior members of the community to respond to reports of security vulnerabilities and who operate using private channels of communication. Besides working to resolve known security vulnerabilities the Security WG will also operate in a pro-active manner, reviewing existing tools and services from a security perspective; defining Sakai security requirements; devising QA/testing models that identify potential security weaknesses; producing security-related documentation; and helping educate developers on web-related security vulnerabilities.

SECURITY DOCUMENTATION

Public information regarding security vulnerabilities will be documented in security advisories, Sakai software release notes and readme files included in demo, binary and source distributions as well as online at the following locations:

Sakai Issues Tracking: http://jira.sakaiproject.org/jira/
Sakai Release page: http://source.sakaiproject.org/release/

Release documentation for security updates will identify the Sakai version affected including code branches and provide information on how to close the vulnerability. Security vulnerabilities will be ranked by the threat level index listed below:

Critical Risk

Security vulnerabilities classified as a critical risk involve the possible exposure of data to unauthorized viewing, modification, deletion or acquisition as well as attacks that could result in data corruption.

Major Risk

Security vulnerabilities classified as a major risk involve logical attacks that could compromise the availability of Sakai or otherwise degrade system performance, disrupt or circumvent normal application flow control of Sakai tools and services or use Sakai as a platform for attacks on other systems.

Minor Risk

Security vulnerabilities classified as a minor risk involve threats that (1) can be eliminated by updating existing configuration files to reflect a default secure state (e.g., sakai.properties), (2) are considered extremely difficult for attackers to exploit and/or (3), if exploited, are of minor consequence to the operation of Sakai installations.

SECURITY ADVISORIES

Whenever Sakai security vulnerabilities surface, the Sakai Foundation will execute a three-step security advisory protocol in order to alert (1) Sakai Foundation partners and designated security contacts associated with known Sakai implementations, (2) the wider Sakai Community, and (3) the public at large regarding security issues.

The first step in our protocol involves providing alerts to our partner institutions and organizations as well as to our security contacts throughout the Sakai Community via the use of private communication channels. We delay deliberately the issuance of community-wide and public security advisories in order to allow time for security updates to be devised, tested, distributed and, if necessary, applied to Sakai installations that are known to the Foundation. Once these systems are patched the wider Sakai Community is alerted and time provided for Sakai implementers unknown to the Foundation to identify themselves, designate security contacts, and patch their systems before we proceed to the third and final step in our security advisory protocol, the general public announcement.

SECURITY CONTACTS

The Sakai Foundation encourages institutions and organizations that download and install Sakai software to consider contacting the Foundation and providing the name(s) and contact details of one or more individuals to serve as security contacts. Security contact information should be emailed to security@sakaifoundation.org.

As noted above, Sakai security contacts receive security updates in advance of public release in order to permit their institution or organization time to patch their Sakai installation before any Sakai security vulnerability becomes general knowledge. Designated security contacts are also provided access rights to view, comment and address issues flagged as security items in Sakai's JIRA issue tracking application. Security-related JIRA issues are hidden from public view. We do not grant access to these JIRA items lightly and we verify the identity and role of each person who is designated as a security contact.

Email traffic sent to sakai-security-contacts@collab.sakaiproject.org should be treated confidentially and should not be forwarded to other Sakai or public email lists or discussed elsewhere in order to help protect institutions and organizations running Sakai from security-related exploits or attacks.