Blackboard Security Testing and Support

https://help.blackboard.com/Learn/Administrator/Hosting/Security/Security_Support

Blackboard performs continuous internal security testing at the code-level (static analysis) and application-level (dynamic analysis) to ensure it meets both Blackboard and our customer's expectations. Furthermore, to regularly get fresh eyes on the application, Blackboard obtains security penetration testing from third party security vendors. Any identified issues are quickly slated for repair.

Static application security testing

Blackboard leverages open source and commercial static analysis scanners to assess Blackboard Learn source code continuously. These tools allow Blackboard to identify potential vulnerabilities in the source code as the system evolves through integration with build environments. Blackboard couples automated source code analysis for security vulnerabilities with manual code reviews.

Dynamic application security testing

Blackboard leverages open source and commercial dynamic analysis scanners to assess the Blackboard Learn application continuously. The automated security scanners test for common web application vulnerabilities from the viewpoint of an end user.

Manual penetration testing

Static and Dynamic Application Security Tools cannot detect all security issues. To further mitigate security risk, Blackboard performs manual penetration

testing to identify more complex security vulnerabilities and business logic issues such as improper authorization.

Security patches and advisories

Blackboard publishes security patches and advisories through Behind the Blackboard.

BbPatch

Customers may install the latest patches using "BbPatch," a package management utility to manage updates to Blackboard products, such as cumulative patches. BbPatch complements the Blackboard Installer by allowing small, reversible updates with minimal downtime.

Software updates

The Software Updates module is located in the Blackboard Learn Administrator Panel and provides updates specific to your Blackboard Learn installation, including Major Releases, Service Packs, and Patch Sets, as well as building block updates and newly released building blocks. The module lists the number of updates that are available. You can select which updates to download.

Security advisories

Blackboard is committed to the timely identification, communication and resolution of security vulnerabilities identified in our products. Security Advisories are released with the following information:

- Advisory ID - for Knowledge Base tracking purposes
- Title - Brief description of affected area
- Issue Date
- Severity

This is followed by a vulnerability overview, which details the nature of the security vulnerability; a functional issue overview which describes how the system may be affected; a list of product version(s) affected; description of discovery; and a description of the solution with a link to applicable patches.

Blackboard also tracks and advises our clients of any known exploitation or malicious use of security vulnerabilities. The mitigations and workarounds section describes any mitigations clients may take or if a workaround is available. If there are multiple revisions to an advisory, a short summary of the update is provided.

Security vulnerability scoring

Blackboard follows the industry standard of CVSSv2 (Common Vulnerability Scoring System Version 2.0) as a guideline. Customers may use our severity ratings as a guideline to help classify the impact of security issues found in Blackboard Learn. It is based on average usage, since not all vulnerabilities have equal impact on all users - for example, customers might not have the affected module enabled, or its use of the module may not contain as critical information as another customer.

Input Validation Filter - Security management building block

The Input Validation Filter acts as a first line of defense with configurable rules to protect Blackboard Learn. It is, in a sense, like a firewall for Blackboard Learn. It verifies that user requests coming in are safe by sanitizing the data through a default ruleset. An advantage of the Input Validation Filter is speed. This feature provides you with cross-site scripting fixes much faster than the traditional patching process. Traditional patches can have various dependency issues or may need to be rolled back. Providing fixes through the Input Validation Filter is a much cleaner and faster way of delivering patches, as they are provided directly through the Software Updates Center.