Print This Article

<< Return to Zero-day holes found in Blackboard platform

Zero-day holes found in Blackboard platform

Darren Pauli, editor, SC Magazine, Australia/New Zealand edition
September 16 2011
Multiple zero-day security vulnerabilities have been found in the world's most popular educational software – holes that allow students to change grades and download unpublished exams, while allowing criminals to steal personal information.

Vulnerabilities in the Blackboard Learn platform have the potential to affect millions of school and university students and thousands of institutions around the world.

The platform is used by the United States military to train soldiers.

After several weeks of investigation by university IT managers, security professionals and *SC Magazine Australia*, Blackboard Learn has acknowledged it is sending a security advisory to customers to address the issue.

Penetration tests

Sources within Australia's university sector, talking to *SC Magazine Australia* on condition of anonymity, believe they may have been first to discover the security holes.

One Australian university, which declined to be named for this story, recruited penetration testing company Securus Global to ethically hack the software.

The security company told *SC Magazine Australia* that its policy was to not disclose any information about clients.

But sources told *SC Magazine Australia* that during tests of the Blackboard software, security professionals had gained administrative access to databases in which student exams, assignments and grades were stored. Personal information stored on students was also accessible.

The problems relate to default configuration and web application vulnerabilities present in all versions of the Blackboard Learn system. The latest version of the platform was thought to make exploitation slightly more difficult, but did not rectify the problems.

University IT managers said they believed most schools and universities using Blackboard would operate the outdated and more vulnerable systems.

Upon *SC Magazine Australia's* initial investigations, Stephanie Tan, Blackboard Learn security director, said the vulnerabilities examined were at that point not “highly critical."

“We are not aware of any institution's academic or student data having been compromised in any way by these issues,” Tan said.

“Many of these issues are common issues associated with any type of web application or software, and all of the issues will be addressed through existing patches and planned releases.”

But Tan confirmed the vulnerabilities would remain unpatched until the first service pack update is delivered “prior to the end of the year.”

University IT managers told *SC Magazine Australia* they would not be able to wait. They became concerned that they would be forced to shut down the systems, disrupting distance and online courses, should the holes be exploited.

Several advised Blackboard Learn of the holes and sought further information on the vulnerabilities. They claim their requests fell on deaf ears for more than a month.

“They didn't want to know about it, which quite frankly, I couldn't believe,” one IT manager of a major university said. “I was stunned.”

Blackboard did not respond when asked to explain why the company ignored customer requests for information.

After weeks of failed attempts to gain information from Blackboard, the problem was escalated to AusCERT, a nonprofit security organization funded by the *University* of *Queensland*.

The industry heavyweight warned Blackboard it would publish an advisory to the Australian security industry and its global network of Computer Emergency Response Teams.

A security adviser at Blackboard, believed to be a different employee than the case handler in the initial round of communication with customers, quickly responded and promised the holes would be addressed.

AusCERT declined to comment for this story, but confirmed it had an advisory ready to be issued.

Response

Blackboard Learn said it would in response issue an advisory on Friday to universities.

“We issued a support bulletin to Blackboard Learn clients today after completing our review of the issues," the company said in a statement. "The bulletin includes information about how the issues are being addressed through existing patches and planned releases, as well as recommendations for general security management and best practices.”

“The majority of the issues were known issues responsibly reported by other institutions and security researchers, and for which Blackboard has commenced remediation for release to the larger client base as part of our standard operating procedure.”

Blackboard said it strove “to be vigilant at building security into its products and providing prompt and carefully tested product updates.”

“When Blackboard learns of any potential vulnerability, we investigate the issue and establish a resolution plan as part of our standard procedure.”

The company said one vulnerability remained to be investigated.

“We are completing our investigation on one remaining issue in collaboration with the institutions who reported it.”

This article originally appeared at SCMagazine.com.au