Security Advisory - LRN-120000 - Malicious OneClass Chrome Extension

Date Published: Dec 12,2016 **Category:** Product:Authentication_and_Security_Learn; Version:Learn_9_1_Q4_2016,X9_1_SP14,Learn_April_2014_9_1_201404_160205,Learn_October_2014_9_1_201410_160373,SaaS,Learn_9_1_Q4_2015_9_1_201510_117
Article No.: 000043180

Product: Blackboard Learn

Type: Security Advisory

Bulletin/Advisory Information:

LRN-120000 Malicious OneClass Chrome Extension

Advisory ID	LRN-120000
Title	Malicious OneClass Chrome Extension May Send Email on Students' Behalf and also Attempts to Collect User Credentials
Issue Date	December 12, 2016
Severity	Critical
Products	Affected: Blackboard Learn™, 9.1 Q4 2016 Release and prior and Blackboard Learn™ SaaS.
Version	1.0

Vulnerability Overview

The OneClass Chrome Extension is not available directly via search in the Chrome Extensions Store and students are being phished with the following link to install it:

- https://chrome.google.com/webstore/detail/oneclass-easy-invite/aamdmgbfnjpdfkjjbobpkhnhpcmolpja

During installation, the extension requests permissions to "Read and change all your data on the websites you visit". However, students may not closely read or fully understand the requested permissions before accepting them. The extension adds a button inside the Learn pages to "Invite Your Classmates to OneClass".

The plugin will email all the students in a students' class (utilizing Learn URLs and resources, which are functioning as designed) to promote the OneClass plugin/product. The plugin also has code that attempts to collect and send the users' credentials (both username and password). We are in the process of determining if the code is successful in doing so.

The mail content is:

> "Hey guys, I just found some really helpful notes for the upcoming exams for <University Name> courses at https://oneclass.com/s/signup. I highly recommend signing up for an account now that way your first download is free!"

Affected and Non-affected Products

The following products have been tested to determine which supported versions are affected. To determine the support life cycle for your product and version, visit Behind the Blackboard's Support Services Guide.

Affected Products

Product	Vulnerability	Aggregate Severity Rating
Blackboard Learn™, 9.1 Q4 2016 Release and prior and Blackboard Learn™ SaaS.	Severity: High Impact: Privacy	Critical

Solution

Raise awareness to all users that this extension should not be installed. Blackboard is currently working on mitigating controls and this bulletin will be updated once they are completed.

Fix Versions

No fix is available at this time.

Blackboard Security Commitment

Blackboard is committed to resolving security vulnerabilities quickly and carefully, leading to the release of a Security Advisory and any needed product update for our customers. To best serve our community and to protect our customers and their data, we encourage our customers to confidentially report vulnerabilities to us so that we may investigate and respond expeditiously. Once we have developed and comprehensively tested a remedy, we announce the vulnerability and distribute a product update to licensed customers to help minimize the threat to customers everywhere. Whether publicly or privately communicated, we will work diligently to ensure that any confirmed vulnerabilities are addressed.

Blackboard Learn Vulnerability Management Commitment and Disclosure Policy

References

- Bug Tracking Number:

Vulnerability	Bug Tracking Number
Access Control Vulnerability in Content Area Could Allow	LRNSI-24146 LRNSI-24115

Information Exposure	LRN-120000

Revision History

Version	Date	Description
1.0	December 12, 2016	Advisory Published

Support

Blackboard is happy to speak with any customers directly regarding this advisory. Customers may contact Client Support using the local toll-free number or submit a case through Behind the Blackboard.

Disclaimer

Statements regarding our product development initiatives, including new products and future product upgrades, updates or enhancements represent our current intentions, but may be modified, delayed or abandoned without prior notice and there is no assurance that such offering, upgrades, updates or functionality will become available unless and until they have been made generally available to our customers.

The information provided in this advisory is provided "as is" without warranty of any kind. Blackboard disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Blackboard or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Blackboard or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.