REN-ISAC

2022-Sep-26

Advisory: D2L Brightspace Abused for Email Fraud

Sharing Guideline: TLP:WHITE

Executive Summary

Default configurations of the Learning Management System (LMS) D2L Brightspace do not throttle outgoing email. Cybercriminals are taking advantage of compromised institutional accounts and this default behavior to launch high-volume email attacks like phishing from the Brightspace LMS.

Further Details

The email tool within Brightspace and its default configuration offers few meaningful constraints against its use as a platform from which to launch bulk email attacks against user groups internal and external to an organization. Additionally, because cloud hosted instances of Brightspace use D2L's email infrastructure, any settings in the institution's email service to mitigate high-volume outgoing email traffic are bypassed.

The following are specific settings that help mitigate this issue:

- d2l.Tools.Mail.RestrictContactsToAvailableCourses
  - When set to **on**, this restricts the set of contacts that are shown in the email address book when the user filters by "All Contacts." These restrictions prevent contacts from being displayed in inactive courses, courses that have not reached their start date, and courses that have passed their end date.
  - Scenario: When a person composes an email from the Email tool and selects "All Contacts" using the Address Book, the course classlist does not display if the course is inactive, past the end date, or not yet begun.
- d2l.Tools.Mail.RestrictContactsByAddressBookOn
  - When set to **on**, this restricts the set of contacts that are shown in the email address book when a user filters by "All Contacts." This restriction prevents contacts from courses where the address book is disabled from being displayed.
  - Scenario: When a person composes an email from the Email tool and selects contacts using the Address Book, a course classlist does not display if the course Address Book is disabled.
- d2l.Tools.Mail.MaxToCCAddresses
  - When set to a positive integer (e.g., **200**), this setting restricts the maximum number of addresses in the TO or CC fields. A value of **0** means **unlimited** recipients.
  - Scenario: If set to the default 200, when a person composes an email from the Email tool and inserts 201 or more addresses into the To or CC field, a message pops up stating: *There were 1 error(s) found in the information you submitted: There are more than 200 recipients in the To or CC field and your email will not be sent. Please move recipients to the BCC field.*

Figure 1 Graphical user interface error depicting one too many email addresses set in the TO or CC fields

- d2l.Tools.Mail.MaxBCCAddresses (new setting established in May 2022)
  - When set to a positive integer (e.g., **200**), this setting restricts the maximum number of addresses in the BCC field. A value of **0** means **unlimited** recipients.
  - Scenario: If this is set to the default of 200, when a person composes an email from the Email tool and inserts 301 or more addresses into the BCC field, a message pops up stating: *There were 1 error(s) found in the information you submitted: There are more than 200 recipients in the BCC field and your email will not be sent.*

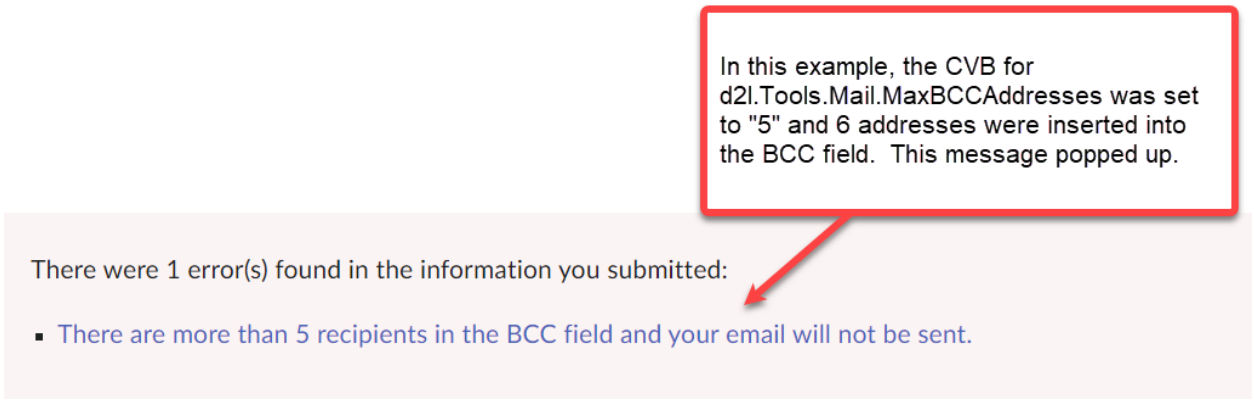

Figure 2 Graphical user interface error depicting one too many email addresses set in the BCC field

- d2l.Tools.Mail.MaximumNumberOfIndividualAddresses
    - When set to a positive integer (e.g., **100**), this setting restricts the maximum number of addresses that can be displayed in one field before they are collapsed into a single bulk field.
    - Scenario: If this is set to 100, when a person composes an email from the Email tool and inserts 101 or more addresses into a field, the individual addresses will not display in the field. Instead, a single entry will display in the field showing the number of recipients such as *101 recipients*. The message will be sent, and the Sent Mail message will display the individual recipient names and email addresses.

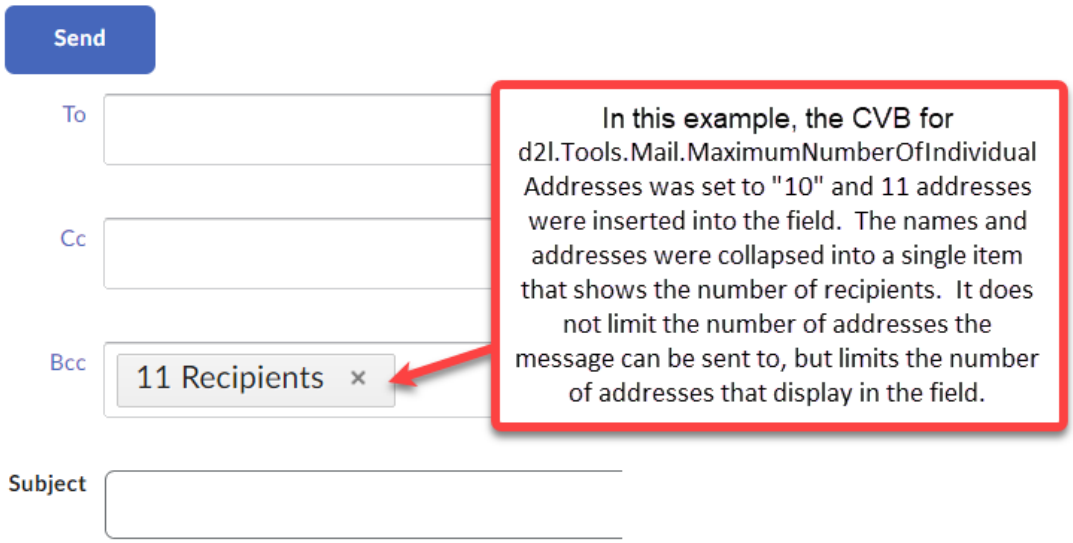

Figure 3 Graphical user interface depicting a list of email addresses collapsed into a single recipient that simply says, "11 Recipients"

It's also possible to configure the following Email tool permissions on a role basis:

- Access Email
- See the Address Book
- Create Personal Contacts in Address Book
- See the Role Names in the Address Book
- Send Emails to External Email Addresses
- Send Attachments
- See External Email Addresses for 'Student'
- See External Email Addresses for 'Instructor'

If an institution's Brightspace instance uses roles broken down by groups such as per-course, per-department, or per-institution; it may be beneficial to disable permission at an institutional level and re-enable by a more granular role like course.

Additionally, for courses defined to have large enrollments, one may consider disabling the following Tools:

- Classlist
- Discussions
- ePortfolio
- Groups*
- Office365

* Note: the Groups tool cannot be turned off. However, it is possible to adjust the course navbar to one that does not display the Groups tool link.

Communications Template

The following may be used as a template to communicate any changes to a local institutional audience.

From: <CISO>
To: <CIOs>
Cc: <Learning Technology>; <Student and Academic Services>; <Others as Appropriate>
Subject: Changes to Email Functions in D2L Brightspace, Effective Immediately

Colleagues,

In collaboration with D2L, <Institution> will be implementing changes to the email functions available within campus Brightspace sites. These changes will be made so emails sent from the Brightspace email tool will only be delivered to classlists or members of current active courses for all users. D2L and <Institution> are making this change to reduce the possibility of unsolicited messages being sent out in bulk (e.g. phishing) from Brightspace.

This change will not impact those emails sent via Brightspace notifications. Email functions generated by <Institution> remain unchanged.

Additional controls to email will be made to a limited number of Brightspace course sites that contain a classlist with an entire student population (e.g. all first year students, etc.). In these instances, email functions will be limited only to those with the role of an instructor/faculty member.

Please contact me if you have any questions.

Acknowledgments

Thanks to the Minnesota State Colleges and Universities system for liaising with REN-ISAC on this issue and providing Brightspace expertise. Thanks also to them for their internal communications that they allowed us to use as a draft for this advisory.