Published on *University of Colorado* (https://www.cu.edu)

Multipronged approach prevents data breach [1]

March 29, 2022 by UIS Communications [2]

On Dec. 11, 2021, just as students were preparing for final exams, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a statement on a global security threat known as the Log4j vulnerability and urged all public and private entities to attempt remediation.

At the University of Colorado, the Office of Information Technology [3] (OIT) on each campus and University Information Services (UIS) were aware and already working to prevent a data breach. Thanks to connections between the Office of Information Security and several higher education security consortiums, CU learned of the vulnerability and immediately got to work on collaborative solutions.

Brad Judy, director of information security, explained, “Timing is crucial. Because the higher ed community shares information freely, and because we at CU have been participating in information security collaboration for years, we learned right away.”

A multipronged strategy

Log4j is a ubiquitous widget often included in bundles within applications, so the first challenge was identifying all its instances. While teams went to work on that issue, others tackled the configurations needed, which kept rapidly changing daily.

Adding to the complexity, many applications containing Log4j were commercial software packages. In that case, product managers had to reach out to vendors for patches to securely update applications. UIS, Advancement IT and campus OIT teams worked collaboratively throughout the process, developing secure, alternative solutions.

Judy praised UIS and campus OIT teams for their tactical work and coordination efforts, which allowed Judy’s team to focus on monitoring and protecting CU’s systems.

As winter break approached with a still dynamic situation, CU leaders decided to put extra protection in place to forestall an emergency over the break. Students, faculty and staff were required to be on a CU network to access affected applications, which meant using a CU Virtual Private Network (VPN) for those who were remote.

Restricting access to only those on a CU network limited the risk temporarily. It also required collaboration and communication with all members of CU, many of whom had never previously logged in to a CU VPN. Faculty entering final grades and students registering for spring classes needed clear instructions. Service Desks, business offices and departments across campuses responded to the challenge. Previous work establishing multifactor verification also helped.

Art Figel, UIS director of student IT services, described the work his team did to mitigate the disruption. “We needed everyone’s help and participation – including students-,” he said. “It was a big ask during a critical time, but everyone rose to the occasion.”

When Anschutz Medical Campus students found that they couldn’t access the payment page for courses with additional fees, Figel’s team quickly found workarounds.

Monitoring sensors recorded a rate of one attempted attack on CU systems per second.

Safeguarding data

Amid patching and mediation efforts, monitoring sensors recorded a rate of one attempted

attack on CU systems per second. Given the personal identifiable information required for financial aid and the amount of data within CU applications, a breach would have easily cost the university millions of dollars.

Thanks to enormous efforts and an impressive level of collaboration, CU did not experience a data breach due to Log4j.

Associate Vice President and Chief Information Officer Scott Munson credited the cross-campus team effort. “I’m incredibly grateful for the talented people across our campuses and system office. The trusted partnerships we have built over the years enabled us to effectively work through an incredibly dynamic and complex situation that impacted all of us,” he said.

Increasing cybersecurity efforts

Unfortunately, cybersecurity work is never finished. New threats are always in the works. Munson emphasized the need for proactive work, saying, “Staff rallied to save the university from a potentially severe financial loss and protected the data of the people we serve. But we know that attempts to breach security are steadily increasing.”

In the fall of 2021, CU IT Governance [4] approved a systemwide cybersecurity project. This multiyear effort, led by OIS with campus and system IT offices in full support, will not only increase CU’s overall security posture but also enable more proactive steps to secure the CU environment.

“The time we have to react keeps decreasing, so we have to drive proactive work as well as the efficiency of reactive work,” Judy said.

According to Judy, this will require more resources and a culture of putting security first.

“Cybersecurity is everyone’s responsibility at CU.”

cybersecurity [5], OIT [6], IT Governance [7]
Display Title:
Multipronged approach prevents data breach
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/uis-news/multipronged-approach-prevents-data-breach
[2] https://www.cu.edu/blog/uis-news/author/65709
[3] https://www.cu.edu/security
[4] https://www.cu.edu/it-gov
[5] https://www.cu.edu/blog/uis-news/tag/cybersecurity
[6] https://www.cu.edu/blog/uis-news/tag/oit
[7] https://www.cu.edu/blog/uis-news/tag/it-governance