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

Protecting university operations: Why some security updates can’t wait. [1]

October 19, 2026 by ES and UIS Communications [2]

Advances in artificial intelligence are changing how software companies identify security vulnerabilities, leading to more frequent critical security updates. At the same time, cybercriminals are using AI to identify and exploit security weaknesses, increasing the urgency of addressing security risks. For UIS, these developments mean responding quickly to emerging threats while minimizing disruptions to university operations when possible.

AI is changing how vulnerabilities are discovered and exploited

In recent months, major software companies, including Oracle, Microsoft and Google. have incorporated AI into their vulnerability detection processes, helping identify security weaknesses that may have previously gone undetected. As a result, critical security updates may be released more frequently.

However, software companies aren't the only ones using AI. Cybercriminals can also use AI to identify vulnerabilities and accelerate attacks, potentially reducing the time organizations have to address security weaknesses before they are exploited.

While improved detection helps UIS address potential security risks, the growing speed of cyberthreats makes timely patching more important than ever.

“Our responsibility is to protect the systemwide administrative systems and System Administration IT services that support the university’s daily operations. When a critical vulnerability emerges, acting quickly, even when it requires brief, unscheduled maintenance, can prevent a longer outage, protect sensitive data and preserve trust in the services our students, faculty, and staff rely on. We will make these decisions carefully and communicate as clearly and promptly as possible,” said Scott Munson, Chief Information Officer.

Responding quickly to emerging threats

Unlike work performed during UIS’ planned monthly maintenance windows, critical security patches may require immediate attention, leaving less time to schedule updates in ways that minimize disruption to normal business operations. As AI-driven vulnerability detection and cyberthreats continues to evolve, UIS anticipates that emergency maintenance with little advance notice may become more frequent.

“While this may be inconvenient for users, it’s critical we step in as soon as possible to deploy these patches,” said Sridevi Bankupalli, UIS director of Enterprise Development. “Otherwise, our systems may be susceptible to major breaches.”

Stay informed with Maintenance Matters and RAVE alerts

When emergency patches are necessary, UIS will communicate them as soon as possible through the RAVE alert system [3] and the UIS Maintenance Matters blog [4].

Although critical security patches may occasionally cause service interruptions, these updates are essential to reducing risk and protecting university data and systems.

Send email when Published:
No

Source URL:https://www.cu.edu/blog/uis-news/protecting-university-operations-why-some-security-updates-can%E2%80%99t-wait

Links
[1] https://www.cu.edu/blog/uis-news/protecting-university-operations-why-some-security-updates-can%E2%80%99t-wait [2] https://www.cu.edu/blog/uis-news/author/249473 [3] https://www.cu.edu/uis/uis-service-desk/emergency-alerts [4] https://www.cu.edu/uis/maintenance-matters