INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

Action required: Spring4Shell exploit

April 6, 2022

You've received this email because you're subscribed to UIT's public email list.

A new zero-day exploit called Spring4Shell affects the popular Spring Framework and results in remote command execution on vulnerable systems. This serious vulnerability is easy to exploit on any network-visible software that uses that framework, and is being aggressively exploited across the internet.

IT system owners at the University of Utah must examine their systems or work with their vendors to determine if their software is using the vulnerable framework.

- https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965

If you have questions, please contact VulnerabilityManagement@iso.utah.edu.

IT system administrators should join the Spring4Shell vulnerability Teams channel (login required) for more information and discussion about what other colleges and orgs are doing to protect themselves and the U against the vulnerability.

Share this email:

Manage your preferences | **Opt out** using **TrueRemove**™
Got this as a forward? **Sign up** to receive our future emails.
View this email **online**.

University of Utah - UIT 102 S 200 E Ste 110
Salt Lake City, UT | 84111 US

This email was sent to .
To continue receiving our emails, add us to your address book.

Subscribe to our email list.