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

If you have questions, please contact [VulnerabilityManagement@iso.utah.edu](mailto:VulnerabilityManagement@iso.utah.edu).

IT system administrators should join the [Spring4Shell vulnerability Teams channel](https://teams.microsoft.com/l/channel/59763141c1ad4638a89272dfac747c50/Team%20-%20Spring4Shell%20vulnerability%20management) (login required) for more information and discussion about what other colleges and orgs are doing to protect themselves and the U against the vulnerability.