



Urgent reminder for IT admins: Service inventory required to assist Log4Shell mitigation efforts

January 31, 2022

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

Following up on a [previous announcement](#), university leadership would like to remind IT administrators at the U of the urgent need to provide a service-level inventory for all websites, network-accessible applications, and embedded systems within their colleges, departments, and organizations.

Please complete this [service list template in Box](#) (login required) and email it to log4jreporting@utah.edu, making sure to include:

- Service name
- College/department/organization
- Point of contact
- Internet accessible: Y/N
- Notes on vendor-provided vulnerability/remediation status

Please be prepared to work quickly with your dean or director to provide the needed information. If needed, the Information Security Office will escalate to the dean or director to assure timely responses.

Going forward, please email updates or status changes from vendors to log4jreporting@utah.edu so that mitigation efforts can be tracked.

IT administrators also are strongly encouraged to join the [Log4Shell vulnerability Teams channel](#) (login required) as soon as possible to stay updated on ongoing vulnerability and mitigation efforts.



Node 4 story idea? Email us:
stratcomm@it.utah.edu



it.utah.edu

[NotifyIT](#) | [Follow us on Twitter](#) | [IT Services Status](#) | [IT Service Portal](#)

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.