INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

# *Log4Shell vulnerability memo to Council of Academic Deans*

**December 16, 2021**

---

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

We'd like IT administrators at the U to be advised that CIO Steve Hess is sending a memo to Council of Academic Deans members regarding the urgent need to provide a contact list for IT systems, servers, websites, apps, and IoT devices within their colleges and orgs. **The contact list (login required) is due as soon as possible, by Tuesday, December 21, 2021.** The memo content is provided below for your preview. 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.

We encourage you to join the Log4Shell vulnerability Teams channel (login required) as soon as possible to stay updated on the vulnerability and mitigation efforts.

---

**To:** Council of Academic Deans
**From:** Steve Hess, CIO
**Subject:** Urgent: IT contacts and app/system inventory for your org needed ASAP

A very serious IT security vulnerability known as Log4Shell has recently been identified as a global threat to institutions, businesses, and Internet of Things (IoT) devices. Log4Shell is one of the most severe internet threats in history, in part because of how simple it is for anyone with internet access to exploit, enabling infiltration and control of network-connected applications, IT systems, servers, websites, and IoT devices.

Unfortunately, like thousands of other organizations globally, the University of Utah is vulnerable to exploitation. **We must rapidly respond to protect our data, IT services, and systems.** While we've been able to address the vulnerability in centrally managed IT systems (e.g., Canvas, Box, CIS), we have no inventory of individually or locally managed IT systems, websites, and apps to verify they are not affected or are patched appropriately.

**We're particularly concerned about research lab/group IT systems and apps, which may be managed by a PI, postdoc, or graduate student rather than the designated IT manager for the college or org.**

To enable the Information Security Office to verify that your local systems and apps are protected, **as soon as possible please use the attached spreadsheet to document the following IT information for your college or org:**

- **Contact information** (name, uNID, email address, phone number) for everyone in your college or org who manages network-connected applications, systems, servers, websites, and IoT devices.
    - *IMPORTANT: This should include research labs/groups that manage their own specialized IT systems, devices, webpages, and applications.*

Please return your org's spreadsheet as soon as possible this week or **before Tuesday, December 21, 2021, to log4jreporting@utah.edu.**

UIT will follow up with your IT contacts about how to check their systems and attest that they are not affected or have been patched. In the meantime, IT system administrators should join the Log4Shell 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.

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

***it.utah.edu***

**NotifyIT | Follow us on Twitter | IT Services Status | IT Service Portal**