INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

Major security flaw discovered in Drupal core

You are receiving this email because you are subscribed to UIT's public email list.

Note: *This message is also being sent to NotifyIT security, infrastructure, and applications subscribers via email.*

Summary

Drupal recently issued an advisory about a highly critical remote code execution flaw in the Drupal core that can lead to arbitrary PHP code execution. If exploited, it could allow criminals to inject code to hijack sites or servers, phish user credentials, or spread malware.

Impact

The University of Utah's Information Security Office is aware of the issue and is closely monitoring developments. Drupal has released security updates, as well as information about other ways to mitigate the risk.

Recommendations

Users should ensure their devices are up to date with currently-available upgrades. Users also can disable all web service modules or configure their web servers to not allow PUT/PATCH/POST requests to web services resources.

More information

- http://bit.ly/Drupal-advisory
- http://bit.ly/threatpost-drupal-flaw

If you have questions or need assistance, please contact your respective help desk: UIT Help Desk at 801-581-4000, option 1; ITS Service Desk at 801-587-6000.

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

it.utah.edu

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