Information Security Office
Office of Information Technology

ISO Position Paper

Position Title	Emergency Vulnerability Patching
Position Audience	Princeton IT Professionals
Contact	Information Security Office: InfoSec@princeton.edu
Position Release Date	November 15, 2016
Last Update	Initial posting

Problem Statement

Security vulnerabilities for information systems and applications are announced on a regular basis by vendors and third parties. The University successfully mitigates many vulnerabilities through regularly scheduled, non-emergency measures. However, there are occasions where the severity of a published vulnerability, coupled with a broad exposure to potential exploits of that vulnerability, warrants immediate action at the direction of the ISO.

ISO Position

The ISO will review published vulnerability information on its own and in collaboration with University colleagues on a regular, ongoing basis. When it is determined that a published vulnerability presents an immediate risk to University information categorized as Restricted or Confidential[1], the ISO will inform the University technical community (e.g., IT managers and SCAD/DCS) of the necessity to apply a vendor provided patch or to employ some other suitable risk mitigation as appropriate within one (1) week of the communication from the ISO regarding the vulnerability. Due to current policy, architectural and design constraints, the ISO will consider the general population of systems on campus as potentially having or enabling access to Restricted and Confidential data thus requiring patching broadly across the environment.

Appropriate channels will be used to alert the University technical community to the necessary actions, and follow-up scanning for mitigation will be conducted by the ISO Security Engineer(s).

Additional Information

Vulnerability management should be done on all systems and applications on an appropriately routine basis. The ISO recommends at least a quarterly patch cycle for University resources. A monthly patch cycle is strongly encouraged in the case of Restricted and Confidential data.

All systems and application should be managed for vulnerabilities on a routine basis.

Information Security Office
Princeton University

[1] Information Security Policy

Data classification: Public