RISE
Enable • Protect
Research-centric Information Security Enablement Program

# BSD Information Security Office Cybersecurity Newsletter

December 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 12


***Inside this Issue:***



## SA&A System Accreditation

**Have you ever asked?**

- Is my **existing or new system** secure?
- Is my research data safe?
- How do I obtain security configurations for grants or IRB approval?

If so, the BSD Information Security Office (ISO) can assist you with identifying security requirements with your project and ensure that these systems are protecting your data through the Security Assessment and Authorization (SAA) service.

**For a list of systems currently enrolled in the SAA process, visit:**
http://security.bsd.uchicago.edu/saa_review

**Wondering how to submit a system for review?**
Contact the BSD ISO directly via security@bsd.uchicago.edu for anonymous &

confidential submissions and questions.

For additional information, refer to the BSD SAA landing page: http://security.bsd.uchicago.edu/bsdsaa

# Information Security Enhancements & Changes to Access

The Organizations' Information Security Offices have teamed up to enhance the overall security posture. To protect against known risks, the following enhancements are being made.

| What | Why | What to Do | When |
|---|---|---|---|
| BSD Clinical Networks will be blocked for direct remote access | A risk to the clinical operations of UCM exists due to this direct access. Will be applying the Server firewall zone policy (login with CNETID or UCHAD) | Leverage Cvpn, BSD VPN or UCM VPN to access your desktops remotely | Start 12/30/2016 End 1/6/2017 |
| UCM Remote Citrix will require two factor authentication before accessible outside of the UCM network | Phishing attacks have raised in prevalence, with ~15% of UCM/BSD being susceptible. This can permit remote attackers access to sensitive data in Citrix. 2FA ensures your account is secure even if your password is compromised | Enroll in two factor authentication at http://2fa.uchicago.edu to maintain access | 12/30/2016 |
| Devices on BSD Networks will be routinely scanned for basic security hygiene for remote access services. | Cyber-attacks on remote access services (e.g. RDP, VNC) have become more prevalent and periodic scanning is a basic security hygiene process to identify system weaknesses before systems are compromised. | Use strong passwords for remote access services or limit access to cVPN, BSD VPN or UCM VPN | 1/4/2017 |
| UCM VPN will require two factor authentication before accessible outside of the UCM Network | Phishing attacks have raised in prevalence, with ~15% of the UCM/BSD being susceptible. This can permit remote attacks access to the UCM network. 2FA ensures your account is secure even if your password is compromised | Enroll in two factor authentication at http://2fa.uchicago.edu to maintain access | Planned 1/13/2017 |

| | | | |
|---|---|---|---|
| UChicago Box will require two factor authentication to login for the BSD | Phishing attacks have raised in prevalence, with ~15% of the UCM/BSD being susceptible. This can permit remote attacks access to sensitive data in Box. 2FA ensures your account is secure even if your password is compromised | Enroll in two factor authentication at http://2fa.uchicago.edu to maintain access | Planned 1/24/2017 |
| Enable a privacy and security control for mobile devices on the University's email system for BSD faculty and staff | Consequences of unencrypted lost data include fines, identity theft, compromised research data, endangered federal grant status, and risk to the reputation and image of the organization. To avoid these issues and align with regulatory requirements, mobile devices connecting to the email system will require encryption. | Encrypt your mobile device before February 28, 2017 | Planned 2/28/2017 |

**FOR MORE INFORMATION OR ASSISTANCE WITH 2FA:** If you are having trouble enrolling or encountering any problems, please contact the ITS Service Desk at 2-5800. Once you enable 2FA for your CNETID and UCHAD you will automatically be protected through a number of sites.

## Remote Desktop Access Vulnerability Detection

Due to recent remote desktop cyber security incidents within our organization, the BSD Information Security Office is taking proactive measures to protect devices. Beginning on **January 4th, 2017**, devices on BSD Networks will be routinely scanned for basic security hygiene weakness in remote access services.

The BSD ISO will perform targeted remote desktop and brute force vulnerability scans on the BSD network to identify vulnerabilities associated with popular remote desktop services such as RDP, SSH, VNC, FTP, Apple Remote Desktop, TeamViewer, and PCAnywhere. Periodic scanning is a basic security hygiene process to identify system weaknesses before systems are compromised. These remote desktop services are under continuous attack which can result in the compromise of BSD research data, endangered federal grant status, fines, identity theft, and risk to the reputation and image of the organization.

**How will this impact you?**
Users will be able to utilize remote services during the vulnerabilities scans and should see no service interruption.

**Do you need to notify anyone?**
System Owners and IT Custodians have been made aware and will be notified

again prior to the start of scans.

**What if a vulnerability is found?**
If a vulnerability is found, the BSD ISO will contact the department's BSD IT Custodian to resolve the issue as soon as possible. If vulnerability is not handled the network port of the system will be shut down.

**Can I opt out of having my devices scanned?**
To prevent scanning, devices can be moved behind the University of Chicago border firewall policy that prevents access from the Internet.

As best practice, IT Custodians should perform the following to prevent vulnerabilities:

- Restrict remote desktop protocol by implementing host-based firewalls on all endpoints vulnerable to this attack. Users will no longer be able to directly connect to their work computers here on campus without first establishing a VPN connection.
- Enforce the use of strong passwords.
- Keep system software up to date.
- Read and follow the BSD Minimum Security Standards for Systems and the BSD Guidelines for Securing Devices located on the BSD ISO website (security.bsd.uchicago.edu) and click on Security Policies.

**What to do if you become aware of an information security incident?**

**Contact the BSD ISO Team via email at security@bsd.uchicago.edu.**