INFORMATION ASSURANCE

"Confidence in Cyberspace"

INFORMATION ASSURANCE ADVISORY NO. IAA U/OO/803537-16 **Date: 3 January 2017**

SUBJECT: Reduced the Risk of Vulnerabilities in Unix®[1]/Linux®[2]-Based Operating Systems

DISCUSSION:

Unix®/Linux® is a family of operating systems that underpin a large portion of government and commercial servers and infrastructure devices. Due to the prevalence of Unix®/Linux® systems in public and private infrastructure, and the existence of many exploits and implants that are available, ensure system security by following community best practices and understanding current threats and risks.

As general guidance, as well as their accompanying software and services, update and patch all deployed Unix®/Linux® systems to the latest supported versions. Additionally, enable system and network auditing so that servers and systems detect anomalies, attacks, and intrusions quickly.

MITIGATION ACTIONS:

For Unix®/Linux® systems, NSA recommends the following general mitigations that would make exploitation and implantation more difficult or detectable:

- Operating System
  - Apply all available patches
  - Upgrade to the latest supported version, or at least a supported version:

Red Hat®[3]Enterprise Linux®	7 (latest) or 6
IBM®[4] AIX®[5]	7.2 TL0 (latest) or 7.1 TL4
Oracle Solaris®[6]	11 (latest) or 10
Hewlett Packard®[7] HP-UX®[8]	11i v3 (latest) or 11i v1/v2
FreeBSD®[9]	11

  - Disable all unneeded services
- Third-Party Software
  - Apply all available patches to installed software
  - Upgrade to the latest supported version, or at least a supported version
- Networking
  - Ensure Local Area Network (LAN) protocols, for example Server Message Block (SMB) and Remote Procedure Call (RPC), are blocked at gateways
  - Limit remote administrator access conducted through Secure SHell (SSH)
  - Limit administrative access to specific Internet Protocol (IP) addresses
  - Use an out-of-band management network where possible
  - For systems requiring legacy software/kernel versions, avoid connections with untrusted networks and tightly restrict and inspect traffic through a firewall and/or proxy
- SELinux®[10]

    - Enable enforcing mode for SELinux® — if this is not possible, then enable permissive mode for SELinux® so that access violations are logged
- Continuously monitor systems for anomalous accesses and command-line activities

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

FOR FURTHER INFORMATION, PLEASE CONTACT

Industry Inquiries
410-854-6091A
email: bao@nsa.gov

Client Requirements and General Information Assurance Inquiries
IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov

[1] Unix is a registered trademark of The Open Group.
[2] Linux is a registered trademark of Linus Torvalds.
[3] Red Hat is a registered trademark of Red Hat, Inc.
[4] IBM is a registered trademark of International Business Machine Corp.
[5] AIX is a registered trademark of International Business Machine Corp.
[6] Solaris is a registered trademark of Oracle Corp.
[7] Hewlett Packard is a registered trademark of Hewlett Packard Corp.
[8] HP-UX is a registered trademark of Hewlett Packard Corp.
[9] FreeBSD is registered trademark of The FreeBSD Foundation.
[10] SELinux is a registered trademark of the National Security Agency.