INFORMATION ASSURANCE

"Confidence in Cyberspace"

CYBER TECHNICAL BULLETIN **Date: 13 DEC 2017**
NO. CTB U/OO/229250-17

SUBJECT: Securing Kernel Modules on Linux Operating Systems

DISCUSSION

The Linux®[1] kernel is the core component of a family of Operating Systems (OS) that underpins a large number of government and commercial servers and infrastructure devices. Kernel functionality is commonly enhanced through the use of modules, which can be loaded at boot time or during normal system operation. Modules run at the same privilege level as the kernel. Any vulnerabilities in kernel modules present a serious risk.

System owners are advised to 1) ensure that only signed kernel modules are loaded, and 2) prevent loading of unnecessary kernel modules. Although it reduces attack surface, preventing module loading is not practical for many general-purpose systems and thus is not suitable for use in compliance baselines.

MITIGATION ACTIONS

Ensure that Only Signed Kernel Modules are Loaded

Configuring the system to load only modules with a valid digital signature makes it more difficult for an attacker to introduce a malicious kernel module to the system. An adversary could use a malicious kernel module to control the system or persist across reboots.

Activating UEFI Secure Boot is necessary to ensure that only signed kernel modules can be loaded. This requires a UEFI-compliant platform configured in UEFI native mode (not legacy or compatibility modes). On most new hardware platforms, including workstations and servers, Secure Boot is enabled in firmware and already pre-configured for select Linux distributions. The exact location of the Secure Boot setting varies by vendor. Once enabled, Secure Boot creates an integrity chain at boot by verifying signatures of firmware, bootloader(s), and Machine Owner Key (MOK). The kernel, initial filesystem, and kernel modules are then verified by this MOK, which is distributed with Secure Boot-ready Linux distributions. Components with untrusted or absent signatures are denied from execution by Secure Boot policy.

Secure Boot support is not integrated into all Linux® distributions. For example, Red Hat Enterprise Linux® (RHEL) version 7 is the only version of RHEL®[2] that has a full Secure Boot signature chain[1]. Likewise, some third-party products include unsigned modules or build their kernel modules at installation time and thus cannot sign them with a vendor's secure private key. Enabling Secure Boot may prevent some products from loading, could affect system functionality, and may require custom configuration[2].

Prevent Loading of Unnecessary Kernel Modules

[1] Linux is a registered trademark of Linus Torvalds
[2] Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc.

Most major Linux® distributions include a large number of modules that provide a wide range of functionality. Most required modules are loaded at boot, but over time, as additional features are exercised, additional modules can be automatically loaded. Reduce the system's attack surface by limiting the available modules only to those needed.

Note that this configuration is only likely to be practical for specialized systems. General-purpose systems often require the ability to load kernel modules on an as-needed basis, in order to interact with new file systems, specialized hardware, or communications protocols.

To disable module loading, run the following command:

```
# sysctl kernel.modules_disabled=1
```

To persist this setting across reboots, create a service that starts on boot that sleeps for a period long enough to initialize vital services and applications and then runs the command listed above[3]. The following file is an example of a *systemd* service that disables module loading after all services are started on boot.

```
# /etc/systemd/system/disable-module-loading.service
[Unit]
Description=Disables loading of kernel modules
[Service]
Type=idle
ExecStart=/sbin/sysctl kernel.modules_disabled=1
ExecStop=/bin/false
[Install]
WantedBy=multi-user.target
```

Once module loading is disabled, it cannot be re-enabled without disabling the service and rebooting, as shown below.

```
# systemctl service disable disable-module-loading && reboot
```

Some modules which are needed for system operation may have normally been loaded during system operation, and not at boot. To ensure these modules are available, they must be loaded at startup prior to when loading is disabled. To load these modules, list them in a file located in */etc/modules-load.d*. For example, the following file explicitly loads the *udf* and *squashfs* modules.

```
# /etc/modules-load.d/critical-mods.conf
udf
squashfs
```

APPLICABILITY:
This Bulletin is issued under the authority defined in National Security Directive 42 [3] and applies to all Executive Departments and Agencies, and to all U.S. Government contractors and agents who operate or use National Security Systems (NSS) as defined in CNSS 4009[4].

REFERENCES:
[1] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-signing-kernel-modules-for-secure-boot

[3] Usually persistent kernel parameters are stored in */etc/sysctl.d*; however, parameters stored here are applied very early in the startup sequence, before many necessary modules are loaded, making it unsuitable for this particular parameter.

[2] https://access.redhat.com/articles/1180943
[3] National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” dated July 5, 1990.
[4] CNSS Instruction No. 4009, “National Information Assurance Glossary,” dated April 26, 2010.

DISCLAIMER OF WARRANTIES AND 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:
Client Requirements and General Information Assurance Inquiries
Information Assurance Requirements Center
410-854-4200
Email: P611_civ@nsa.gov