NATIONAL SECURITY AGENCY
CYBERSECURITY INFORMATION

LIMITING PTRACE ON PRODUCTION LINUX SYSTEMS[1]

INTRODUCTION

The Linux®[2] kernel is the core component of a family of operating systems that underpin a large portion of government and commercial servers and infrastructure devices. Due to the prevalence of Linux systems in public and private infrastructure, ensuring system security by following community best practices to address current threats and risks is critical.

In Linux, *ptrace* is a mechanism that allows one process to “trace” the execution of another process. The tracer is able to pause execution, and inspect and modify memory and registers in the tracee process: in short, the tracer maintains total control over the tracee. The legitimate use case for this functionality is debugging and troubleshooting. Utilities like *strace* and *gdb* use ptrace to perform their introspection duties. Not surprisingly, malicious implants sometimes use this functionality to steal secrets from another process or to force them into serving as proxies for anomalous behavior.

PROPOSAL

Production systems rarely need to use debugging utilities. For this reason, it is often safe to remove the ability to perform ptrace-related functions, at least in normal operational mode. The YAMA Linux Security Module, included in most Linux distributions, can be used to remove the ability for any process to ptrace another. To configure systems to automatically do this on boot, create a service file in */etc/systemd/system* with the following contents:

```
[Unit]
Description=Removes, system-wide, the ability to ptrace
ConditionKernelCommandLine=!maintenance

[Service]
Type=forking
Execstart=/bin/bash –c “sysctl -w kernel.yama.ptrace_scope=3”
Execstop=

[Install]
WantedBy=default.target
```

Ensure that the service file created has read and execute permissions for the owner and group.

After creating the service file with the correct permissions, run the following command as root:

```
systemctl daemon-reload
```

This command registers the service with the Linux initialization process *systemd*. Upon the next boot, tracing will be completely disabled—this also means the strace and gdb utilities will be non-functional. To re-enable these utilities, initiate

[1] The information contained in this document was developed in the course of NSA’s cybersecurity mission including its responsibilities to identify and disseminate information on threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-enabled products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders.

[2] Linux is a registered trademark of Linus Torvalds

a reboot. During boot, edit the kernel arguments to include the value ‘maintenance’.

Once troubleshooting is finished, disable ptrace immediately by running the following command:

```
sysctl -w kernel.yama.ptrace_scope=3
```

APPLICABILITY

This Cybersecurity Information sheet is issued under the authority defined in National Security Directive 42 and applies to all Executive Departments and Agencies and U.S. Government contractors who operate or use National Security Systems (NSS) as defined in CNSS 4009.

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 necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

CONTACT INFORMATION

Client Requirements and Inquiries or General Cybersecurity Inquiries
CYBERSECURITY REQUIREMENTS CENTER (CRC)
410-854-4200
Cybersecurity_Requests@nsa.gov