UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00240

HEAP OVERFLOW LINUX KERNEL BUG

DATE ISSUED: 25th January 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

This nasty Linux bug exists in the legacy_parse_param in the Linux kernel's fs/fs_context.c program which is a parameter used during superblock creation for mount and superblock reconfiguration for a remount which results memory being allocated beyond its bounds.

BREAKDOWN

A calculation performed in legacy_parse_param() "PAGE_SIZE – 2 – size" mistakenly made an "unsigned type" resulting in a large value of "size" having a high value instead of the expected negative value allowing data to be copied beyond the allocated memory slab. Local attackers may exploit the bug to elevate their privileges using triggers to cause the memory overflow and from there may be able to execute arbitrary code. The CVSS rating assigned to this vulnerability is 7.7 making it a "high-security" vulnerability. The CAP_SYS_ADMIN privilege must be enabled for this exploit to be possible and by opening filesystems not supported by the File System Context API, forces the system to use legacy handling.

REMEDIATION STEPS

- Patch Linux systems to be up-to-date for the latest available version – this will also close the Linux 5.1-rc kernel flaw.
- Disable namespaces by setting user.max_user_namespaces
  - RedHat:
    - echo "user.max_user_namespaces=0" > /etc/sysctl.d/userns.conf
    - sysctl -p /etc/sysctl.d/userns.conf
  - Ubuntu and related distributions:
    - sysctl -w kernel.unprivileged_userns_clone=0

REFERENCES & RESOURCES

ZDNet https://www.zdnet.com/article/nasty-linux-kernel-bug-found-and-fixed/