U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00159

LINUX SYSTEMD ROOT SECURITY BUG

DATE ISSUED: 21st June 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Patches have been issued for the notorious systemd Linux bug that allowed unauthorised users to run privileged processes and gain root access to the system using Polkit.

BREAKDOWN

Systemd uses polkit in the place of the sudo command to escalate privileges of users and grant access at a root level for unauthorised users, allowing them to execute commands and run processes they would not normally be able to. The bug was discovered 7 years ago CVE-2021-3560 and a patch released this month. It is difficult to detect anomalous behaviour relating to this vulnerability as the polkit uses dbus-daemon for the User ID of the requesting process numerous time over varying codepaths to find one that incorrectly handles an error and must be disconnected at just the right moment to trigger the vulnerable codepath so the request is not rejected by a correct codepath.

REMEDIATION STEPS

- Apply the latest security patches across Linux machines, as this vulnerability affects a number of distributions, particularly newer versions. Upgrade to polkit 0.119 or later.

REFERENCES & RESOURCES

ZDNet	https://www.zdnet.com/article/nasty-linux-systemd-root-level-security-bug-revealed-and-patched
The Register	https://www.securityweek.com/linux-systemd-gives-root-privileges-invalid-usernames
GitHub	https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/