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

CYBER GUIDANCE ISSUE 00242

MAJOR VULNERABILITIES DISCOVERED IN LINUX

DATE ISSUED: 14th February 2022

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

OVERVIEW

Two flaws discovered in the Control Web Panel (CWP formally known as CentOS) web hosting management software could be chained together and exploited to allow code execution as a root user (CVE-2021-45467 – file inclusion vulnerability & CVE-2021-45466 – file write bug). Additionally, a major memory corruption vulnerability in Linux PolicyKit (now known as Polkit) dubbed "Pwnkit" has been discovered after 12+ year of existence (CVE-2021-4034).

BREAKDOWN

Some parts of the CWP in CentOS, Rocky, Alma and Oracle Linux versions are exposed without authentication in the Webroot. While there isn't a huge amount of exposure, if an attacker wished to inject malicious code remotely, all they would need to do is alter an "include statement" to insert the content of one PHP with another before the server runs the executable. To get there, an attacker would need to bypass other security protections to reach the restricted API section by registering a malicious "authorised_keys" using the file-write flaw. Octagon researchers were able to reverse the patch installed to mitigate tis issue and exploit some servers during their tests.

Polkit is installed by default in every major Linux distribution and Qualys researchers have discovered a vulnerability in their tests against Ubuntu, Debian, Fedora and CentOS that allows an ordinary user to gain full root privileges on unpatched machines. This vulnerability has existed since Polkit's inception in May 2009 and while it is technically a memory corruption vulnerability "it is exploitable instantly and reliably in an architecture-independent way." This flaw is able to be exploited even if the polit daemon is not running and with the program being one of the key components for controlling system-wide privileges in any Unix-like operating system and facilitates communication between non-privileged and privileged processes – which can lead to exploitation in experienced hands.

REMEDIATION STEPS

- After backups and testing, update your Linux distribution as soon as possible to the latest version.

REFERENCES & RESOURCES

ThreatPost https://threatpost.com/wordpress-insecure-plugin-rest-api/177866/
Octagon https://octagon.net/blog/2022/01/22/cve-2021-45467-cwp-centos-web-panel-preauth-rce/
ZDNet https://www.zdnet.com/article/major-linux-policykit-security-vulnerability-uncovered-pwnkit/