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

CYBER GUIDANCE ISSUE 00098

LINUX SUDO BUG STILL EXISTS 10 YEARS ON

DATE ISSUED: 2nd February 2021

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

OVERVIEW

Any local user can gain root access privileges using the Sudo command when interacting with Linux and Unix systems. Dubbed "Baron Samedit" CVE-2020-3156, this vulnerability has existed for 10 years now and affects a vast number of distributions of the Operating System software.

BREAKDOWN

The Sudo utility that is built into most distributions of Unix and Linux allows the escalation of user privilege to run a program without the requirement of additional credentials to allow such an action. In some distributions the local user is able to achieve full root access and privileges. While this vulnerability is not remotely exploitable and does require pre-existing access to be considered vulnerable. This low complexity, local attack may be exploited by malicious insiders or human error or poor judgement. Patches should be applied immediately to prevent a heap-buffer overflow attack or exploitation from something more sinister such as the FreakOut malware and Botnet.

REMEDIATION STEPS

- Patch Sudo utility to version 1.9.5p2 or find the appropriate patch on the sudo website for your implementation.

REFERENCES & RESOURCES

Sudo	https://www.sudo.ws/sudo.html
Threatpost	https://threatpost.com/sudo-bug-root-access-linux-2/163395/
ZDNet	https://www.zdnet.com/article/10-years-old-sudo-bug-lets-linux-users-gain-root-level-access/
Qualys	https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit