Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:128 **19-02-2021**

Name: Sudo Buffer Overflow Vulnerability allowing Linux root-level access (CVE-2021-3156)

Threat Classification: Privilege Escalation

Summary:

It has been reported that a major vulnerability in *sudo,* known as '*Baron Samedit*' has been recently patched with the release of Sudo v1.9.5p2. This vulnerability can be exploited by an attacker who has gained access to a low-privileged account to gain root access, even if the account is not listed in */etc/sudoer* - a config file that controls which users are allowed access to sudo commands. It impacts all Sudo installs where the sudoers file (/etc/sudoers) is present which is usually found in most default Linux+Sudo installs.

For more details, please visit following official links:

- https://www.sudo.ws/stable.html#1.9.5p2
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156

Recommendations:

- It is highly recommended to upgrade your sudo package to latest stable release i.e. **1.9.5p2**.
- Update all software including Operating Systems, Servers, web browsers etc to the latest and stable versions with appropriate patches.
- Maintain and implement a strong password policy throughout the infrastructure.
- Regularly maintain data backups and also ensure that backups are stored offline at a secure site.
- Install, regularly maintain and update Antivirus solution from a well reputed vendor.
- Execution of unsigned executables from sensitive webservers and endpoints must be blocked.
- Regularly provide Cyber security awareness sessions for employees and continuously arrange capacity building of the relevant technical resources.
- Do not download attachments from emails unless they are from the trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.