Warning! Unprivileged Linux Users With UID > INT_MAX Can Execute Any Command

December 06, 2018 Mohit Kumar

(https://1.bp.blogspot.com/-hSUGT0NjjZQ/XAlIMJbrsPI/AAAAAAAAyyo/wU40_RnZrso3Dsb_6_16ZVIGPLrjAxfQACLcBGAs/s728-e100/linux-policykit-vulnerability.png)

Hold tight, this may blow your mind…

A low-privileged user account on most Linux operating systems with UID value anything greater than 2147483647 can execute any systemctl command unauthorizedly—thanks to a newly discovered vulnerability.

The reported vulnerability actually resides in PolicyKit (also known as polkit)—an application-level toolkit for Unix-like operating systems that defines policies, handles system-wide privileges and provides a way for non-privileged processes to communicate with privileged ones, such as "sudo," that does not grant root permission to an entire process.

The issue, tracked as CVE-2018-19788 (https://gitlab.freedesktop.org/polkit/polkit/issues/74) , impacts PolicyKit version 0.115 which comes pre-installed on most popular Linux distributions, including Red Hat (https://access.redhat.com/security/cve/cve-2018-19788) , Debian (https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=915332) , Ubuntu (https://people.canonical.com/~ubuntu-security/cve/2018/CVE-2018-19788.html) , and CentOS.

The vulnerability exists due to PolicyKit's improper validation of permission requests for any low-privileged user with UID greater than INT_MAX.

Where, INT_MAX is a constant in computer programming that defines what maximum value an integer variable can store, which equals to 2147483647 (in hexadecimal 0x7FFFFFFF).

So it means, if you create a user account on affected Linux systems with any UID greater than INT_MAX value, the PolicyKit component will allow you to execute any systemctl command successfully.

Security researcher Rich Mirch, Twitter handle "0xm1rch (https://twitter.com/0xm1rch) ," has also released a proof-of-concept (https://github.com/mirchr/security-research/blob/master/vulnerabilities/CVE-2018-19788.sh) (PoC) exploit to successfully demonstrate the vulnerability that requires a user with the UID 4000000000.

Red Hat has recommended system administrators not to allow any negative UIDs or UIDs greater than 2147483646 in order to mitigate the issue until the patch is released.

Have something to say about this article? Comment below or share it with us on Facebook (https://www.facebook.com/thehackernews) , Twitter (https://twitter.com/thehackersnews) or our LinkedIn Group (https://www.linkedin.com/company/the-hacker-news/) .

-->