COMSEC Group
Cyber & Information Security

Dirty Cow - Unauthorized Access

Issue Date: 17/11/2016

Author: Dan Gurfinkel

Comsec Group
Yegia Kapayim St. 21D
P.O.Box 3474, Petach-Tikva
Israel 49130

Prepared by:
Dan Gurfinkel
T: +972 (0) 39234646
E: dang@comsecglobal.com

1. Introduction

Software security updates address faults and missing controls in software, and are implemented in order to fix vulnerabilities in the software. Thus, one of the most important aspects of security is the usage of the most up to date software and services.

This document described two high risk vulnerabilities found in Linux systems.

2. CVE-2016-5195

Privilege Escalation Exploit

Two years ago the ShellShock vulnerability was discovered: a remote code execution exploit in bash that existed for about **25 years** until discovered. While some thought that very old bugs do not exist anymore in Linux, a new vulnerability, known as Dirty Cow, proves us wrong.

This exploit allows local privilege escalation on almost all Linux distributions and kernels as the vulnerable code existed **since 2007** (from kernel version 2.6.22). While this is only a privilege escalation vulnerability, there are already reports of users gaining limited access to servers and using this vulnerability to escalate their privileges.

In fact, the exploit became public as a security researcher observed the exploit in a pcap file.

Prospect clients are urged to upgrade their kernel version as soon as possible.

If you are using an Android device you might need to patch it as well as this exploit can also be used by a malicious app to gain root access (proof of concept code can be found in the following link: https://github.com/timwr/CVE-2016-5195).

3. CVE-2016-4484

Unauthorized access to a Linux Machine

A known security concept is requiring users to provide a username and password combination before allowing them to access the system. This statement was thought to be true for Linux machines as well.

However, it was recently discovered that systems that use the Cryptsetup utility (for example LUKS) are vulnerable to authentication bypass in an attack that is very easy to implement: all the attacker has to do is press the “Enter” key for about 70 seconds. This would allow the attacker to **gain root permissions** to the compromised machine. This bug was found due to the way that Cryptsetup decrypts passwords while the system is booted, thus allowing a user to retry the password for several attempts.

It should be noted that this exploit can only be locally exploited (the attacker needs to gain physical access to the machine in order to compromise it).

4. About Comsec

Comsec Group, founded in 1987, is a pioneering market leader, providing all-inclusive Cyber and Information Security services to clients around the globe. Our mission is to serve our clients as trusted advisors, by securing their information and operational assets, ensuring the achievement of their business goals.

For three decades our unique talent base, professional excellence, deep technical capabilities and access to cutting edge technologies, has enabled us to assist a wide range of leading organizations overcome their security challenges. As an industry leader, we constantly expand the scope of our services and cultivate the unique skills and expertise of our talented experts who are graduates of Israel's elite Cyber Intelligence & Defence Units.

We act as trusted advisor to clients operating in a wide range of industries including, global financial institutions, e-commerce, government agencies, technology, communication and the healthcare sector.

With 140 security experts, we offer a wide range of services, best of breed capabilities, creative mind-set and an extremely quick and flexible response time.

We continually strive to maintain our position as a thought leader in the Information Security arena and stay abreast of the latest security threats and trends. With offices in London, Amsterdam and an Excellence Center in Tel Aviv, Comsec supports pan-European and global corporations. Our innovative services are provided globally to over 600 clients, across 5 continents.

30 YEARS
OF EXCELLENCE

ELITE CYBER
INTELLIGENCE & DEFENSE

600 CLIENTS
ACROSS 5 CONTINENTS

GLOBAL REACH
& OPERATION

"We believe that the role of information security is to enable business growth. At Comsec we are constantly looking for the synthesis of security into the business requirements. Our deep industry and business understanding enables us to tailor our services to facilitate specific business requirements.