|  |  |
| --- | --- |
| Course | Operating System Security |
| Assignment | Assignment 1 |
| Student ID | 100899259 |
| Student Name | Maisha Khatoon |

# Linux Server Vulnerability

## A general description of the vulnerability

The "Dirty COW" vulnerability, also known as CVE-2016-5195, is one common vulnerability affecting Linux servers. It was discovered in 2016 and has an impact on the Linux bit, a crucial component of the operating framework.

The Linux bit's handling of duplicate on-compose (COW) jobs creates a race condition that results in the Dirty COW vulnerability. By using a flaw in the COW component to alter read-only memory pages, attackers can use this vulnerability to get root-level access to a Linux server.

## How would an organization identify this vulnerability?

An organization can identify this vulnerability by using security tools that can spot unauthorized changes to the Linux component or by directing vulnerability outputs. Also, system administrators should keep an eye out for any unexpected activity on their Linux servers, such as shocking cycles or modifications to the structure's documents.

## What are the consequences of this vulnerability being exploited?

Extreme results could result from this vulnerability being exploited, since attackers could control the vulnerable Linux server, gain access to sensitive data, or introduce malware. Moreover, this flaw can be used to gain prestige and defeat security measures like firewalls and access controls.

## How is this vulnerability effectively patched?

Associations must make sure that the most recent component updates are installed on their Linux Servers to successfully patch this issue. In October 2016, the Dirty COW vulnerability was patched, and Linux distributions like Ubuntu, Debian, and Red Hat have released updates to fix it.

In addition to repairing, organizations should think about taking other security measures to protect their Linux Servers against anticipated attacks. This can include limiting client privileges with access controls, running interruption detection systems to look for suspicious activity, and using network division to stop malware from spreading in the event of a break.

Regular security audits and vulnerability assessments can also help identify potential holes in a Linux Server's security posture, enabling organizations to take proactive measures to reduce the risk of double-dealing.

In conclusion, the Dirty COW vulnerability poses a major risk to Linux servers, and organizations should take proactive steps to identify and patch this vulnerability to protect their systems from anticipated attacks. Associations can reduce the risk of double-dealing and reduce the impact of potential security breaches by exercising caution and making serious safety efforts.

# Windows Server Vulnerability

## A general description of the vulnerability

One common Windows Server vulnerability is the "EternalBlue" vulnerability, which was discovered in 2017. It affects the Microsoft Windows operating system and enables attackers to spread malware throughout an organization without interacting with clients.

The Microsoft Server Message Block (SMB) standard, which is used for file and printer sharing on Windows networks, is vulnerable, and EternalBlue makes use of it. Attackers can exploit this vulnerability to get remote access to the vulnerable framework and run erroneous code by sending a specially prepared package to an unpatched Windows Server.

## How would an organization identify this vulnerability?

An organization can identify this vulnerability by using network watching tools that can see suspicious traffic associated with SMB traffic or by directing vulnerability outputs. In order to reduce the risk of double-dealing, Microsoft has also provided a security patch that addresses this issue that can be installed on vulnerable frameworks.

## What are the consequences of this vulnerability being exploited?

Extreme consequences could arise from this vulnerability being exploited, since attackers could use EternalBlue to propagate malware and obtain unauthorized access to sensitive data. The renowned WannaCry ransomware attack in 2017, which affected more than 200,000 PCs in 150 countries, really used the EternalBlue adventure.

## How is this vulnerability effectively patched?

Associations should make sure that all affected Windows Servers are equipped with the latest security update installed to effectively patch this vulnerability. Microsoft's Walk 2017 security update, which can be downloaded and executed from their website, includes a remedy for EternalBlue. Also, organizations should make sure that their systems are constantly updated with the latest security updates to prevent against future vulnerabilities.

Therefore, it is advised that organizations implement additional security measures, such as network segmentation and access controls, to limit the impact of such attacks. Regular security training for employees can also help prevent successful attacks by raising awareness of phishing scams and other common attack vectors.

Overall, the EternalBlue vulnerability poses a major risk to Windows Servers, and enterprises should take proactive steps to identify and patch this vulnerability to defend their businesses from potential attacks. Associations can reduce the risk of double-dealing and diminish the impact of any security breaches by exercising caution and implementing robust safety measures.