

Internal Memorandum

To: Paula Alexander (hal.cio@seccdc.org)

CC: judge\_10@seccdc.org

From: hal10@seccdc.org

Date: February 18, 2019

Memo #: 001

Re: Top System Vulnerabilities

Hello,

As per your request, system vulnerability scans have been performed on our email server, ecommerce site, and Active Directory/DNS servers with Nmap as well as analysis from members of our team. Below, the top three vulnerabilities that were found for each system are outlined.

**AD / DNS:**

1. Zone Transfers

**Issue:** Zone transfers are currently allowed from all systems on the network, allowing anyone to replicate DNS databases.

**Resolution:** The system administration team can restrict the zone transfers to only be allowed from another DNS server on our network.

2. User Accounts with Simple Passwords

**Issue:** Current user accounts on the local system have easily passwords that can be easily cracked.

**Resolution:** This can be resolved by enforcing a strong password policy on the domain and having users change their current passwords.

3. Eternal Blue SMB Exploit

**Issue:** The system is vulnerable to SMB exploit MS17-010, commonly known as Eternal Blue.

**Resolution:** An update for this vulnerability can be applied through Windows Update or a specific patch can be for this exploit.

**E-Commerce:**

1. Shellshock Bash Vulnerability

**Issue:** The currently installed version of Bash is vulnerable to CVE-2014-6271, commonly known as “Shellshock”, which allows for remote code execution.

**Resolution:** This issue can be remediated by updated the installed version of Bash running on the server using the package manager.

2. Apache Denial of Service Vulnerability

**Issue:** The currently installed version of the Apache webserver is vulnerable to CVE-2017-7668 which can be used by an attacker to cause a segmentation fault.

**Resolution:** This can be resolved by updating the version of Apache that is on the system.

3. Linux Privilege Escalation Vulnerability

**Issue:** The version of the Linux kernel on this system is vulnerable to CVE-2016-5195, commonly known as “Dirty Cow”. This vulnerability can be used by an attacker to escalate privileges.

**Resolution:** This vulnerability can be remediated upgrading the version of Linux that the server is running using the package manager.

**Email:**

1. Apache Denial of Service Vulnerability

**Issue:** Apache version 2.2.9 is vulnerable to CVE-2011-3192, which can be used to cause a denial of service.

**Resolution:** This vulnerability can be remediated by updating the version of Apache that is running on the server.

2. Apache Privilege Escalation Vulnerability

**Issue:** Apache version 2.2.9 has a vulnerability that allows low privileged users to gain local administrator rights.

**Resolution:** This vulnerability can be remediated by updating the version of Apache that is running on the server.

3. Dovecot Denial of Service Vulnerability

**Issue:** Dovecot version 1.0.15 is vulnerable CVE-2009-3235 which can lead to a denial of service attack and arbitrary code execution.

**Resolution:** This issue can be resolved by updating the version of Dovecot currently running on the system.

Regards,

Team 10

*In accordance with HAL Memorandum policy, the entire header must be completed or the recipient may not acknowledge this as an official memorandum. Professional communications methods and decorum must be observed at all times.*