July 2014

State of Security

Top Five Critical Issues Affecting Servers

Decisive Security Intelligence You Can Use

Cyber security has never been more important in the quest to defend and protect sensitive information and national security. With information security breaches on the rise and new vulnerabilities developing every day, it is imperative that organizations are adequately informed to defend against top threats.

At Digital Defense, Inc. (DDI), a leading risk assessment company, our Vulnerability Research Team (VRT), works diligently to inform clients of the threats and critical issues affecting servers. This team of certified Security Analysts are thought leaders, highly trained to provide Decisive Security Intelligence to help lock down networks for companies of all sizes and industries. DDI's VRT has provided the analytic expertise necessary to quickly identify zero-day issues in widely used platforms such as Dell EqualLogic Storage Solution, VMware, NovellGroupWise, IBM® WebSphere® Application and many more.

This team of experts is led by Michael Cotton, Vice President, Research and Development for DDI. Cotton oversees development, engineering, and sustaining programs. He is called upon frequently to provide insight surrounding information security issues, presenting at major industry conferences such as RSA and other security venues including BSides, ILTA and ISSA.

In this report, Mike Cotton and his VRT team provide intelligence on the state of security and the top five critical issues affecting servers, and offer recommendations and Decisive Security Intelligence to mitigate risk and bolster security.

Table of Contents

Introduction

With the release of the critical OpenSSL Heartbleed flaw and the impact it had on organizations and industries of all sizes, DDI's Vulnerability Research Team is providing an examination of commonly seen critical security issues that could post a threat by affecting servers and damaging the overall security posture of the targeted organization.

The data identified represents intelligence gathered from the combination of DDI's Vulnerability Research team and our patent-pending scanning technology delivered through a proprietary cloud-based vulnerability management platform. Through intelligent scanning and Decisive Security Intelligence, DDI is able to identify risk trending and provide analysis. This intelligence exposes the top vulnerabilities trending now and presents ways to mitigate risks.

All vulnerability data portrayed within the report was gathered via the Digital Defense Frontline™ Solutions Platform Active View workflow management system. The data represents vulnerabilities discovered in prior vulnerability scans or penetration tests and merged into the workflow management system for assignment to organizations' employees or third-party vendors for actions as part of their remediation activities.

Top Five Critical Issues Affecting Servers

The following are the *Top Five Critical Issues Affecting Servers*.

1. SSL Connection: Server Vulnerable to Heartbleed Attack

Overview:

OpenSSL is used by over 60% of websites worldwide to encrypt personal data. [1]

The SSL Heartbleed flaw was a 'once-a-decade' critical security flaw that will have a lasting impact for years to come. Because OpenSSL is so widely used in various software and hardware applications, nearly all organizations were impacted in some way. The flaw is caused by errors in the memory padding mechanic of the OpenSSL libraries' Heartbeat message, which created a condition that allows remote and unauthenticated attackers to read arbitrary system memory. This flaw can compromise almost every aspect of affected applications.

In the words of Bruce Schneier: ***"On a scale of one to ten, this is an eleven."*** [2]

Even though early reports tended to focus on the potential for SSL certificate theft, a far more critical issue, DDI immediately notified its client base of the leaking of valid VPN credentials on OpenSSL based VPN devices out to the internet. This also affects UDP based DTLS VPNs that public SSL Heartbleed tests were not available for.

From DDI's extensive testing experience, the team believed that VPN credentials were much more readily available than private key certificate data and had the potential for full on data breach impact. This real world scenario has now been confirmed in forensic analysis by security incident response teams.

Methods to Mitigate Risk

Organizations need to understand several things when properly mitigating the Heartbleed flaw:

I. Perform a comprehensive network-based Security Risk Assessment.

Many affected software and hardware vendors released confusing or even inaccurate statements in the wake of the OpenSSL Heartbleed disclosure, which left users wondering what hardware and software was affected.

Network based vulnerability testing of your entire network can quickly remove all doubt about which systems are truly affected and remove the need to have network administrators comparing spreadsheets to various vendor advisories.

II. Check all SSL enabled protocol vectors - not just webservers.

Most security testing for the SSL Heartbleed flaw focuses on traditional webserver SSL vectors. What was underreported at the time of initial release was that the Heartbleed flaw also affects other network services which transition state from cleartext to encrypted mid connection, such as common email and ftp services. Even UDP based VPN services which make use of the DTLS protocol are affected by this flaw, but this vector is rarely tested by most security audits.

III. Perform recurring testing for SSL Heartbleed - not just a one-time-sweep.

Because many hardware devices are affected, there is the potential for a factory-reset-to-vulnerable-firmware state that happens quite often in production environments. A single factory reset of an SSL-VPN based hardware appliance can lead to a devastating data breach. Scheduling recurring vulnerability scans can quickly highlight any changes to a production environment that reintroduce this critical exposure.

2. IPMI Interface: Cipher Suite Zero Authentication Bypass

Overview:

The IPMI cipher suite zero flaw exposes a network based backdoor in the firmware of popular rackmount server hardware by Dell / HP / IBM and other major vendors that can allow a remote unauthenticated attacker to take complete control of the system by using the out-of-band system management agent to override traditional operating system protections.

The cipher zero flaw arises from a debug protocol mode left in place during the creation of early Intel IPMI 2.0 documentation issued in 2006 era. This flaw was reflected as 'no-encryption, straight-password' but was later clarified in 2009 to be 'no-encryption, no-password'. [3]

Unfortunately, this knowledge gap led to several years of major vendors such as Dell, HP, IBM and others shipping their most popular rackmount servers with a network enabled embedded backdoor in the firmware that has the potential to bypass all security restrictions and controls of the host operating system. What's worse is that our experience as a managed security services provider has revealed that this backdoor is extremely common on production networks but clients are rarely aware of it. For more information, download the RSA Conference 2014 Presentation: Hijacking the Cloud: Systematic Risk in Datacenter Management Networks.

Methods to Mitigate Risks:

1. Turn off networking for the embedded IPMI interface if it is not being used.

For companies that do not use the embedded IPMI interface functionality, the best course of action is simply to disable it. Clients are often surprised when we inform them that there is a DHCP enabled firmware IP address enabled on a critical system that has an access trump over the normal operating system.

2. Turn off the cipher zero backdoor on all IPMI interfaces using ipmitool or ipmiutil.

The IPMI cipher zero flaw cannot typically be disabled through the boot time BIOS or Baseboard configuration tools, but you can use dedicated command line tools such as ipmitool or ipmiutil to manually disable it. This remediation can be performed locally on the affected system or over the network.

3. MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability

Overview:

The MS12-020 Microsoft Security Bulletin[4] addresses a remote code execution flaw that an attacker can trigger by sending in a sequence of specially crafted RDP packets to an affected system. This particular vulnerability is especially important because it affects the Remote Desktop Service which, rightly or wrongly, is often externally accessible on critical systems such as company webservers.

Even though most exploitation toolkits have not achieved reliable remote code execution of the MS12-020 flaw, numerous POC's exist which can trivially blue-screen the entire server just by sending a couple of packets at it, leading to a severe disruption of service for all services running on the affected system.

Methods to Mitigate Risks:

System administrators must ensure that all systems are regularly updated for security patches, even those in the DMZ which they are loathe to reboot to install a critical patch. Often times the DDI Vulnerability Research Team witnesses situations where client machines are part of a well maintained patch management process, but heavily firewalled server systems are, paradoxically, more neglected.

While it is not recommend to use RDP on any externally facing server, sometimes there is a business need for this. Regular security assessments can help highlight systems that fall out of alignment with security update procedures.

4. Website Blind SQL Injection Detected

Overview:

While organizations continue to be much better at detecting and eliminating more traditional SQL Injection attacks which directly return data or detailed error messages, we still see quite a bit of Blind SQL Injection vectors when performing vulnerability assessments and penetration testing on new web applications.

Advances in exploitation technology have made blind SQL injection nearly as bad as normal SQL injection in practice. Attackers can use advanced web hacking toolkits to leverage any true/false condition obtained through blind-SQL injection to quickly dump sensitive information from the back end database.

Methods to Mitigate Risks:

- Train developers to use prepared statements or parameterized queries.
- Perform routine code audits of all database-enabled applications.
- Enforce white list input validation for all user input.
- Make use of web application firewalls for external systems.

5. Easily Guessable SSH Credentials

Overview:

SSH password guessing attacks are certainly one of the oldest and most well-known remote-attack vectors, but they continue to remain effective a surprisingly high amount of the time. If you are running an externally facing SSH server and check the system logging, you're almost guaranteed to see random password guessing attempts in your system logs every week using standard common account names (root, guest, admin, etc.).

From our professional experience, the attacks which focus on the root or admin account rarely succeed, but those which use an extended list of well known, less privileged accounts, will more often gain a foothold on a server that can then use one of many recent local-user privilege escalation exploits to gain full admin level access.

Methods to Mitigate Risks:

I. Disable password based access and use SSH cryptographic keys for access.

Public key SSH authentication authenticates users using public key cryptographic keys and is considered industry best practice after initial node setup. Password based authentication can then be turned off in the sshd_config configuration file.

II. Ensure that all service accounts are locked and set to no login shells where possible.

Often software installation on Unix systems requires the creation of user accounts which often fall victim to password guessing attempts. Even services which do not have default passwords will become weak points if people use example passwords provided in popular tutorials. By setting the login shells of any restricted accounts to '/bin/false', you can ensure that even a successful auth attempt will not grant the user a command shell.

III. Consider running SSH on an alternate port other than the default of port 22.

While changing the default SSH port will not defeat a determined attacker, it does at least remove you from the crosshairs of random SSH password-guessing attacks that constantly sweep the internet. Other critical security issues affecting SSH servers will also benefit from this port change, as attackers tend to focus their efforts on internet-wide sweeps of port 22.

Conclusion

With actionable intelligence and a commitment to security, organizations can establish a culture of security through regular security risk assessments, awareness education and Decisive Security Intelligence. This approach to defending against cyber crime helps to fortify defenses against an unwelcome and devastating security breach.

9000 Tesoro Drive

Suite 100

San Antonio, Texas
78015

Tel 210.822.2645
Fax 210.822.9216

ddifrontline.com

About Digital Defense, Inc.

Founded in 1999, Digital Defense, Inc. (DDI) is a premier provider of managed security risk assessment solutions protecting billions in assets for small businesses to Fortune companies in over 65 countries. DDI's dedicated team of experts helps organizations establish a culture of security through regular information security assessments, awareness education and decisive security intelligence. This proven method bolsters the capability of organizations to reduce risk and keep information, intellectual property and reputations secure. The combination of DDI's certified security analysts, patent-pending scanning technology and proprietary cloud-based vulnerability management system, Frontline™ Solutions Platform, delivers one of the most powerful assessment results and remediation management solutions possible. Contact DDI at 888-273-1412 or ddifrontline.com.

---

[1] http://www.heartbleed.com
[2] https://www.schneier.com/blog/archives/2014/04/heartbleed.html
[3] http://ddilabs.blogspot.com/2013/07/the-backdoor-on-side-of-your-server_2.html
[4] https://technet.microsoft.com/en-us/library/security/ms12-020.aspx