IBM Security Solutions
October 2010

IBM X-Force Threat Insight Quarterly

IBM

Contents

About the report

The IBM X-Force® Threat Insight Quarterly is designed to highlight some of the most significant threats and challenges facing security professionals today. This report is a product of IBM Managed Security Services and the IBM X-Force research and development team. Each issue focuses on specific challenges and provides a recap of the most significant recent online threats.

IBM Managed Security Services are designed to help an organization improve its information security, by outsourcing security operations or supplementing your existing security teams. The IBM protection on-demand platform helps deliver Managed Security Services and the expertise, knowledge and infrastructure an organization needs to secure its information assets from Internet attacks.

The X-Force team provides the foundation for a preemptive approach to Internet security. The X-Force team is one of the best-known commercial security research groups in the world. This group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM security products, and educates the public about emerging Internet threats.

We welcome your feedback. Questions or comments regarding the content of this report should be addressed to XFTAS@us.ibm.com.

The Common Platform of Web Application Attacks

By Michael Montecillo

Introduction

It is an often overlooked fact that Web Content Management Systems (WCMS) serve as a backbone to many of the evolutions in so-called Web 2.0. From Fortune 100 companies, to governments, to personal blog sites, WCMS' are a popular choice for organizations wishing to easily manage dynamic content and quickly integrate constantly changing web technology. However, the adoption of WCMS technology has come with a distinct level of risk. WCMS has increasingly become a security issue for organizations who do not possess security strategies to address WCMS adoption. As a result, WCMS have become a platform for attackers to exploit well-known security vulnerabilities. This article briefly explores the risks inherent within WCMS platforms and some methods with which those risks can be mitigated.

WCMS is Often Overlooked

The reality of the Internet is that it is constantly evolving to be more flashy, functional, and inclusive of people of all technical capabilities. In order to cater to the diverse needs of users as well as meet criteria for business to reduce costs in web application creation and administration, WCMS was born. WCMS platforms such as TYPO3, Joomla!, and Drupal are widely utilized by enterprises, small-to-medium businesses, and non-commercial personal web application hobbyists alike. These platforms also served as the primary product of four of the top ten vendors with the most vulnerability disclosures in 2008 according to the X-Force 2008 Trend and Risk Report. While the top ten list has since shifted, the difficulties faced by WCMS have not. The first half of 2010 has seen significant, widely publicized vulnerability disclosures and security incidents with WCMS.

Unfortunately, WCMS continues to be overlooked as a potential vulnerability vector for organizations. This is largely due to the fact that most organizations simply assess the end product, particularly the web applications managed by WCMS instead of actively researching security issues within the WCMS platform itself. Due to the difficult nature of comprehensively assessing web applications, WCMS vulnerabilities are often not discovered in these assessments. As a result, when organizations are vulnerable to WCMS attacks, the vulnerability itself may go overlooked for long periods of time. This in combination with the relative simplicity of exploiting known WCMS vulnerabilities and the high payoff of leveraging exploited sites to attack visitors has made WCMS a primary target of attackers.

Plugins Present a Significant Issue

Things are not entirely hopeless, however, as many WCMS vendors have taken proactive steps towards delivering more secure products. This includes providing patches for security vulnerabilities, which of course is often difficult to come by when speaking about web application vulnerabilities. Major vendors such as Joomla! and Wordpress deliver WCMS patches through simple to apply updates. Unfortunately, the security of these platforms does not end there.

WCMS platforms allow for third-party plugins to deliver functionality to users. These third-party plugins typically do not undergo the same scrutiny that WCMS base platforms do. In addition, the developers are often not directly affiliated with the base platform organizations. Therefore, the security teams of base platforms find it difficult to track and ensure that all third-party plugins with known issues are secured. Furthermore, there is very little that these vendors can do to secure those plugins. The results of these difficulties can be viewed in Joomla!'s effort to notify their user base of plugins with known vulnerabilities. This effort can be seen on their website in the form of a "vulnerable extensions list" which is a long list of vulnerable Joomla! Plugins.
http://docs.joomla.org/Vulnerable_Extensions_List

How Bad is It?

The first half of 2010 has been a testament to these issues. Web application vulnerability disclosures accounted for 55% of the overall vulnerability disclosures according to the 2010 IBM X-Force Mid-Year Trend and Risk Report. Vulnerabilities in WCMS' and their plugins contributed a large portion to the total number of disclosures. In fact, one particular website which focuses solely on providing exploits for the Joomla! WCMS and its plugins have already had 477 new exploits posted in 2010.

In addition, successful WCMS attack incidents have been amongst the most widely publicized security events of the year. In April, a large scale attack was launched against websites leveraging Wordpress hosted at GoDaddy.com, a large web hosting company. These attacks functioned as a core component in the distribution of malware. The attacks leveraged vulnerabilities in older versions of Wordpress to deliver malicious Javascript code which redirected visitors to malicious sites that exploited various vulnerabilities in the victim operating system or applications and delivered several forms of malware.

The GoDaddy incident was not isolated by any means, however, attacks against WCMS are continually becoming more common. In fact, another extremely similar wide scale successful attack against GoDaddy took place in late September. In addition, automated attacks against WCMS platforms made up a large portion of the web application attack statistics noted in the 2010 IBM X-Force Mid-Year Trend & Risk Report. These statistics are typically harder to create as WCMS attacks usually alert as regular web application attacks. It is not until deeper investigation is conducted that it is discovered that the web application attack was actually directed against the WCMS platform.

Addressing the Issue

On a positive note, addressing WCMS vulnerabilities largely does not require a significant venture from many organizations current security strategies. At their core, CMS' are typically web applications. This means that if they are given the same attention as in-house developed secure web applications, the organizations that deploy them will have the same level of assurance in their security.

If an organization leverages an open-source CMS, conducting Source Code Analysis (SCA) is usually the best way of determining whether vulnerabilities exist. Once vulnerabilities are discovered, there are several options for users. Either the organization can spend the development cycles to implement the solution, or they could report the vulnerability to the vendor as some vendors have security teams that will release a patch for the issue.

Of course, SCA is not always an option as it can be expensive and frankly not all of CMS code is publicly available. Thus, organizations should implement a blackbox web application assessment process as well. However, these assessments must be a little more targeted than typical blackbox web application assessments. Most out-of-the-box commercial web application scanning solutions do not have the capability to target CMS' without special configuration. This means that assessors must focus their automated scanning solutions and penetration testing processes to be inclusive of the underlying CMS. This is especially true for organizations that utilize third-party plugins, as they tend to be the most vulnerable.

Finally, monitoring and protecting CMS can be accomplished with typical web application security countermeasures such as Intrusion Prevention Systems (IPS) and Web Application Firewalls (WAF). Although, alerts in these technologies would most likely not be specific to the CMS' they are protecting. Rather, most of these technologies produce generic alerts such as "SQL Injection" or "Cross-Site Scripting" events detected. Determining whether these alerts are actually detecting attacks specific to CMS' usually require more investigation or custom signatures.

Conclusion

Content Management Systems are quickly becoming a core component for IT operations within businesses and governments of all shapes and sizes. As this technology continues along the technical adoption curve, it is imperative that organizations develop strategies to securely implement and manage the technology. These strategies should include many of the similar processes and procedures that in-house developed web applications utilize.

However, efforts must go beyond merely conducting regular focused assessments to developing methods for fully understanding the threats that organizations face in light of WCMS attacks. The attackers that make up the threat environment are well aware of the difficulties in properly securing WCMS platforms. They have refined methods for exploiting these difficulties and are actively practicing those methods. Unless organizations take a proactive approach to mitigate the risks associated with WCMS adoption, WCMS will continue to be a highly targeted aspect of information technology.

It Isn't Always Cyber

By Michelle Alvarez

Technical threats are abound. Connect a database to a web server, and it's only a matter of time before someone tries to pilfer its contents via SQL injection. Entire enterprises, it seems, can be consumed by the latest botnets. These threats represent just a few of the countless security concerns organizations are currently facing. There is also the increasing pressure to align security practices with compliance requirements and business goals. For years, IBM X-Force Threat Insight Quarterly reports have addressed these topics in an effort to arm readers with an understanding of these technical security threats—botnets, malware, phishing, etc. However, there's another facet to security that should not be overlooked—physical security.

Physical security involves protecting personnel, infrastructure and other assets from physical intrusions. When it comes to gaining unauthorized access, attackers exploiting physical security have as many tricks up their sleeve as cyber attackers. In fact one particular demonstration conducted at the DEF CON® Hacking Conference held this year proved even advanced physical security mechanisms could be circumvented using simple modified keys and key blanks (keys that have not been cut to a specific bitting). The presenters showed that pressing a key to the inside of one's forearm leaves an imprint which can than later be used to create a functional key.

Outside-In

Consider the following scenario. An individual walks into your organization and approaches the front desk. This person gives the security guard a fictitious name and asks that he be paged. While the guard is busy searching for the name in the company's directory, the attacker uses this time to discreetly lean over the desk (pretending to help locate the fictitious employee) and press his wrist on the guard's key. Is it a key that unlocks exterior doors? A server room? Maybe it is a skeleton key that works on several locks. Through a few more social engineering attempts, this malicious individual could potentially gain access to various locations within your facility.

An insider certainly poses a threat since they have an understanding of the company's weaknesses or access to areas that an external person might not be privy to. This gives them an obvious advantage—no need to bypass protection systems to obtain sensitive information. However, as illustrated in the earlier scenario, one can not underestimate the capabilities of an outsider gaining access to a facility and its critical assets.

The results of the Social Engineering Capture the Flag contest held at DEF CON this year clearly exemplified this issue. The contest involved participants using social engineering techniques to obtain information from various targeted companies. Exploitation was successful with every company where the contestant was able to speak with a human representative on the phone. With the information gathered from these types of phone calls, attackers can begin to paint a picture of how they might go about targeting a particular company's physical vulnerabilities.

Rarely does a single attacker do all of the reconnaissance work. Attackers are often part of a larger well-organized, profit driven crime organization. The retail industry is one of the hardest hit by these sophisticated groups. A National Retail Federation survey found that 89.5 percent of retailers surveyed say their company had been a victim of organized retail crime within the past 12 months. These crimes cost retailers nationwide somewhere between an estimated $15 and 30 billion annually.[1]

Physical security also involves protection against physical events. When disaster strikes, there is the obvious concern for employee welfare. Are there any employees located at the facility at the time of the disaster? Is there a rescue effort underway? There should be a plan in place which determines who gets notified in the event of a disaster. The plan should also include the locations of back-up sites.

[1] NRF 2010 Organized Retail Crime Survey http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=940

Natural disasters such as fires, floods, earthquakes, and hurricanes can cause as much of a disruption to business as an attacker and can result in huge monetary loss. The costliest natural disaster in U.S. history, Hurricane Katrina, had a major economic effect on a number of industries that reached into the billions of dollars in damages.[2] These events leave infrastructure and other assets even more vulnerable to physical threats since any barriers that have been put in place may be destroyed or missing.

Mitigating the risk

Since there are different components to the physical threat equation, there are varying methods of mitigation against these types of threats. From environmental design to access control systems, there are number of layers to physical security. Each layer plays a natural role in enhancing an organization's physical security.

When discussing physical security, environmental design most likely comes to mind first. This is basically the makeup of the environment. What are the physical barriers in place to deter an attacker from targeting a particular facility? There should be a fence around the property and warning signs. Metal or concrete barriers could also be used as deterrents. The facility should be appropriately lit at night and entranceways should be clearly visible. The physical make-up of the building is also something to consider. Many buildings now have glass walls on the ground floor. Glass windows should be set with triggers that fire in the event of a break. The idea is to create an environment that is unfavorable to attackers.

Aside from environmental barriers, there should also be mechanical hurdles to jump through. There may be gates, doors, locks, or a combination of these devices. The type of access control implemented determines the level of deterrence. If the organization is small, then key access may be an option. However, with large user populations and high user turnover, key control becomes unmanageable. In this case, organizations may want to opt instead to implement electronic access control. It is also important to consider with both forms of access control the levels of access required for each individual. Should there be restricted access to the area where financial records are kept? Does everyone need access to the server room?

Intrusion detection systems and alarms to monitor and alert on attacks offer additional layers of physical security. Digital security surveillance, such as IBM Physical Security Services—video correlation and analysis suite, can identify patterns and trends in your environment. This allows you to identify and react quickly to anomalies.

Finally, security guards play an important role in all of these areas. They patrol the environment, assist in enforcing policies controlling access, and respond to incidents alerted by the detection systems, video surveillance, and alarms. Security guards help to establish an atmosphere of vigilance. Their very presence is a visible and effective deterrent to many would-be attackers.

In the event of a physical disaster, however, the aforementioned countermeasures may no longer apply. In this scenario, the best defense is to be well-prepared by ensuring there is an up-to-date business continuity and disaster recovery plan in place. Not only should this plan be developed and implemented, but it should also be tested on a regular basis through preparedness exercises. IBM Business Continuity and Resiliency Services can help keep your business operating under virtually any condition, comply with regulations and gain the ability to recover from disasters.

[2] Economic effects of Hurricane Katrina http://en.wikipedia.org/wiki/Economic_effects_of_Hurricane_Katrina#cite_note-1

"Defense In-Depth" Applies

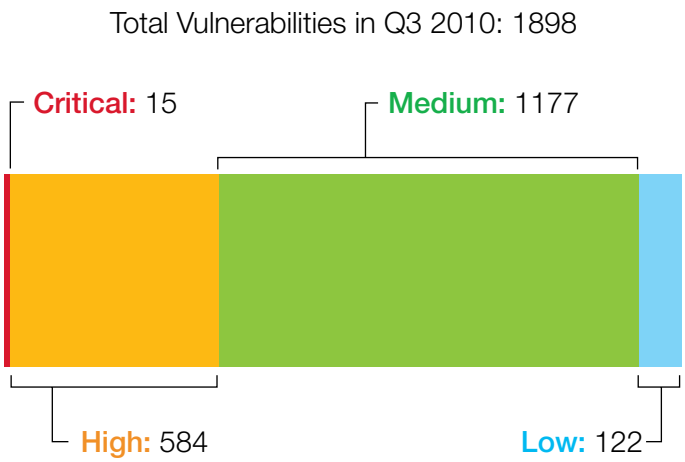
Should the same amount of emphasis be placed on protecting against physical threats as cyber threats? The answer to this question is, absolutely yes. Organizations have no way of knowing where the next attack will come from. The concept of defense-in-depth extends to physical security as well. Security should be addressed from a holistic viewpoint. However, where the security gaps lie will vary from organization to organization. One company may get a gold star in terms of protection against cyber security threats while leaving themselves wide open on the physical front.

Knowing where the holes are in your security posture may require the help of a trained physical security professional. Consulting services, such as Professional Security Services from IBM Security Services, can provide a comprehensive assessment of your current security posture. These consultants have the expertise to advise on which products and services best suit your organization's security needs from a cost and security effectiveness perspective.

Prolific and Impacting Issues of Q3 2010

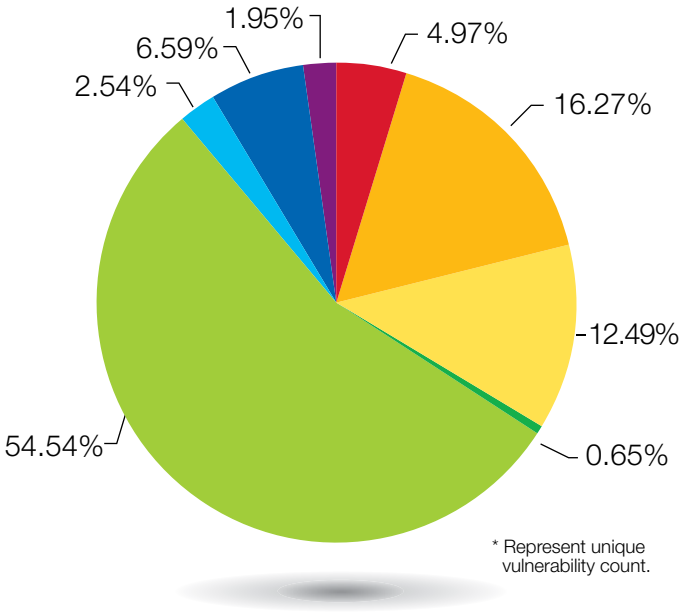
Significant disclosures

In Q3 2010, the X-Force team researched and assessed 1898 security related threats. A significant percentage of the vulnerabilities featured within the X-Force database became the focal point of malicious code writers whose productions included malware and targeted exploits.



Source: IBM X-Force

The chart below categorizes the vulnerabilities researched by X-Force team analysts according to what they believe would be the greatest categories of security consequences resulting from exploitation of the vulnerability. The categories are: Bypass Security, Data Manipulation, Denial of Service, File Manipulation, Gain Access, Gain Privileges, Obtain Information, and Other. *



Source: IBM X-Force

Bypass Security	Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner.
Data Manipulation	Manipulate data used or stored by the host associated with the service or application.
Denial of Service	Crash or disrupt a service or system to take down a network.
File Manipulation	Create, delete, read, modify, or overwrite files.
Gain Access	Obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system.
Gain Privileges	Privileges can be gained on the local system only.
Obtain Information	Obtain information such as file and path names, source code, passwords, or server configuration details.
Other	Anything not covered by the other categories.

The X-Force team published one IBM Protection Advisory and one Protection Alert for vulnerabilities covered in Microsoft's July Security Release. The Protection Advisory addresses an issue, discovered by IBM X-Force, in the accwiz.dll library which ships with Microsoft® Access. Successful exploitation could result in code execution with privileges equal to the Microsoft Office program used as an attack vector. From a targeted attack perspective, the risk of exploitation is quite high—even though multiple steps are required.

- A protection advisory provided by IBM: ACCWIZ Release-After-Free Remote Code Execution Vulnerability[3]
  - IBM Protection Signatures: CompoundFile_ReleaseAfterFree_Exec, JavaScript_NOOP_Sled, JavaScript_Shellcode_Detected
- CVE-2010-1881
- Microsoft Security Bulletin MS10-044: Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335)[4]

The Protection Alert highlights a remote code execution vulnerability affecting all supported versions of Microsoft Office Outlook. By persuading a victim to open an attachment in a specially crafted email message, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim.

- A protection alert provided by IBM: Microsoft Office Outlook Could Allow Remote Code Execution[5]
  - IBM Protection Signature: Content_TNEF_Outlook_Attachment_Exec
- CVE-2010-0266
- Microsoft Security Bulletin MS10-045: Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212)[6]

[3] A protection advisory provided by IBM: ACCWIZ Release-After-Free Remote Code Execution Vulnerability http://www.iss.net/threats/371.html

[4] Microsoft Security Bulletin MS10-044: Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335) http://www.microsoft.com/technet/security/bulletin/ms10-044.mspx

[5] A protection alert provided by IBM: Microsoft Office Outlook Could Allow Remote Code Execution http://www.iss.net/threats/372.html

[6] Microsoft Security Bulletin MS10-045: Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212) http://www.microsoft.com/technet/security/bulletin/ms10-045.mspx

In mid-July, reports began to surface regarding the exploitation of a 0-day vulnerability in the way that Windows Explorer and other file browsers handle malformed .LNK and shortcut files. An attacker could exploit this issue by persuading a victim to attach a USB drive or CD-ROM with a malicious shortcut file or browse to the root folder of the device using Windows Explorer or a similar file manager. Within days of these reports, proof of concept exploit code was made publicly available. The malware Stuxnet as well as several additional malware families began exploiting this vulnerability. Microsoft produced an out-of-band Security Bulletin to address this issue. IBM X-Force released a Protection Alert to highlight product coverage.

- A protection alert provided by IBM: Microsoft Windows Shell Could Allow Remote Code Execution
  - IBM Protection Signatures: HTTP_FileTypeLnk, FTP_FName_Lnk, Email_Executable_Extension, HTTP_Lnk_File_Accessed, Email_Lnk_File_Attachment, FTP_Lnk_File_Accessed, LNK_File_Detected, SMB_Lnk_File_Accessed, LNK_MsWin_Code_Execution
- CVE-2010-2568
- Microsoft Security Bulletin MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)[7]

Microsoft's August Security Release was one of Microsoft's largest releases in the past two years—addressing 34 issues. IBM X-Force released five Protection Alerts to address those vulnerabilities they believed to be most serious.

[7] Microsoft Security Bulletin MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198) http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx

Three of the Protection Alerts address vulnerabilities affecting Microsoft Windows. The most severe of the issues could result in remote code execution. The other two Protection Alerts highlight remote code execution issues affecting Microsoft Word.

- A protection alert provided by IBM: Microsoft Windows TCP/IP could cause Elevation of Privilege[8]
  - IBM Protection Signature: IPv6_Invalid_Hop_by_Hop_Header
- CVE-2010-1892
- Microsoft Security Bulletin MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)[9]

- A protection alert provided by IBM: Microsoft Windows Cinepak Codec Remote Code Execution[10]
  - IBM Protection Signature: AVI_Cinepak_Codec_Exec
- CVE- 2010-2553
- Microsoft Security Bulletin MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)[11]

- A protection alert provided by IBM: Microsoft Windows SMB Server Remote Code Execution[12]
  - IBM Protection Signature: SMB_Trans2_QueryFS_Exec
- CVE-2010-2550
- Microsoft Security Bulletin MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)[13]

- A protection alert provided by IBM: Microsoft Office Word Could Allow Remote Code Execution[14]
  - IBM Protection Signature: RTF_Word_Overflow_Exec
- CVE-2010-1902
- Microsoft Security Bulletin MS10-056: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)[15]

- A protection alert provided by IBM: Microsoft Office Word Could Allow Remote Code Execution[16]
  - IBM Protection Signature: RTF_Word_Memory_Corruption_Exec
- CVE-2010-1901
- Microsoft Security Bulletin MS10-056: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)[17]

8 A protection alert provided by IBM: Microsoft Windows TCP/IP could cause Elevation of Privilege http://www.iss.net/threats/378.html

9 Microsoft Security Bulletin MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886) http://www.microsoft.com/technet/security/bulletin/ms10-058.mspx

10 A protection alert provided by IBM: Microsoft Windows Cinepak Codec Remote Code Execution http://www.iss.net/threats/375.html

11 Microsoft Security Bulletin MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665) http://www.microsoft.com/technet/security/bulletin/ms10-055.mspx

12 A protection alert provided by IBM: Microsoft Windows SMB Server Remote Code Execution http://www.iss.net/threats/374.html

13 Microsoft Security Bulletin MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) http://www.microsoft.com/technet/security/bulletin/ms10-054.mspx

14 A protection alert provided by IBM: Microsoft Office Word Could Allow Remote Code Execution http://www.iss.net/threats/377.html

15 Microsoft Security Bulletin MS10-056: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638) http://www.microsoft.com/technet/security/bulletin/ms10-056.mspx

16 Microsoft Office Word Could Allow Remote Code Execution http://www.iss.net/threats/376.html

17 Microsoft Security Bulletin MS10-056: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638) http://www.microsoft.com/technet/security/bulletin/ms10-056.mspx

On the same day as the aforementioned alerts, X-Force also released a Protection Alert to highlight a remote code execution vulnerability in Adobe® Flash Player. An attacker could exploit this issue via a specially-crafted SWF file to execute arbitrary code on the system Links to a malicious document can easily be sent through spam or through links on seemingly non-malicious Websites.

- A protection alert provided by IBM: Adobe Flash Player Remote Code Execution[18]
  - IBM Protection Signatures: JavaScript_NOOP_Sled, JavaScript_Shellcode_Detected, JavaScript_Large_Unescape
- CVE-2010-0209
- Adobe Security Bulletin APSB10-16: Security update available for Adobe Flash Player[19]

In late August, a remote code execution issue that affects the Apple QuickTime ActiveX control (QTPlugin.ocx) was disclosed. An attacker may embed a browser frame link on an otherwise non-malicious website to an exploit for this vulnerability or try to entice a user to click on a link for example, in an email.

- A protection alert provided by IBM: Apple QuickTime ActiveX control code execution[20]
  - IBM Protection Signature: javascript-large-unescape
- CVE-2010-1818

In early September, reports began circulating of the active exploitation of a 0-day vulnerability affecting Adobe Acrobat and Reader. The Internet Threat Level was elevated to AlertCon 2 to bring awareness to this issue. Soon after reports surfaced, the security tool Metasploit released a module that leverages this vulnerability to create access to remote machines. This increases the chances of exploitation in the wild. This vulnerability could result in remote code execution if a victim opens a specially-crafted PDF (portable document format) file.

- A protection alert provided by IBM: Adobe Reader and Acrobat Remote Code Execution[21]
  - IBM Protection Signatures: OTF_Sing_Overflow, PDF_Encoded_JavaScript_Tag, PDF_Encoded_Filter_Tag, PDF_Obfuscated_Stream, PDF_JavaScript_Hex, PDF_JavaScript_Exploit, JavaScript_Unescape_Obfuscation, JavaScript_NOOP_Sled, JavaScript_Large_Unescape, JavaScript_NOOP_Splitting
- CVE-2010-2883
- Adobe Security Advisory APSA10-02[22]

[18] A protection alert provided by IBM: Adobe Flash Player Remote Code Execution http://www.iss.net/threats/379.html

[19] Adobe Security Bulletin APSB10-16: Security update available for Adobe Flash Player http://www.adobe.com/support/security/bulletins/apsb10-16.html

[20] A protection alert provided by IBM: Apple QuickTime ActiveX control code execution http://www.iss.net/threats/380.html

[21] A protection alert provided by IBM: Adobe Reader and Acrobat Remote Code Execution http://www.iss.net/threats/383.html

[22] Adobe Security Advisory APSA10-02 http://www.adobe.com/support/security/advisories/apsa10-02.html

The September Microsoft Security release contained nine bulletins and covered eleven vulnerabilities. The X-Force team released Protection Alerts for two of the issues they considered most significant. The first issue is in Microsoft's Local Security Authority Subsystem Service (LSASS) and could allow a remote authenticated attacker to execute arbitrary code on the system, caused by a memory corruption error.

- A protection alert provided by IBM: Microsoft Windows Local Security Authority Subsystem Service Could Allow Elevation of Privilege[23]
  - IBM Protection Signature: LDAP_LSASS_Heap_Overflow
- CVE-2010-0820
- Microsoft Security Bulletin MS10-068: Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539)[24]

The second issue affects Microsoft Office Outlook and could also lead to remote code execution. Successful exploitation can be accomplished by convincing users to open an attachment in a specially crafted email message.

- A protection alert provided by IBM: Microsoft Office Outlook Could Allow Remote Code Execution[25]
  - IBM Protection Signature: Content_TNEF_Exchange_Code_Execution
- CVE-2010-2728
- Microsoft Security Bulletin MS10-064: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2315011)[26]

In late September, Microsoft reported seeing limited attacks exploiting a 0-day vulnerability in ASP.NET. An attacker who successfully exploits this vulnerability could read data which was encrypted by the server. This vulnerability can also be used for data tampering. If successfully exploited, this could be used to decrypt and tamper with the data encrypted by the server. Microsoft released its second out-of-bound Security Update for the quarter to address this issue.

- A protection alert provided by IBM: Microsoft Vulnerability in ASP.NET Could Allow Information Disclosure[27]
  - IBM Protection Signature: HTTP_IIS_ASP_WebResource_Fetch_Error
- CVE-2010-3332
- Microsoft Security Bulletin MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)[28]

[23] A protection alert provided by IBM: Microsoft Windows Local Security Authority Subsystem Service Could Allow Elevation of Privilege http://www.iss.net/threats/382.html

[24] Microsoft Security Bulletin MS10-068: Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539) http://www.microsoft.com/technet/security/bulletin/ms10-068.mspx

[25] A protection alert provided by IBM: Microsoft Office Outlook Could Allow Remote Code Execution http://www.iss.net/threats/381.html

[26] Microsoft Security Bulletin MS10-064: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2315011) http://www.microsoft.com/technet/security/bulletin/ms10-064.mspx

[27] A protection alert provided by IBM: Microsoft Vulnerability in ASP.NET Could Allow Information Disclosure http://www.iss.net/threats/384.html

[28] Microsoft Security Bulletin MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure (2418042) http://www.microsoft.com/technet/security/bulletin/ms10-070.mspx

Additional Q3 2010 Quarter highlights

This section of the report briefly covers some of the additional threats facing security professionals during Q3 2010.

Stuxnet Labeled "Hack of the Century"

The Stuxnet malware first came to analysts' attention in mid-July when it was observed exploiting the 0-day Microsoft Windows .LNK/.PIF vulnerability (CVE-2010-2568). News reports then quickly surfaced of a targeted attack against a SCADA (Supervisory Control and Data Acquisition) system utilizing this malware. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory confirming that the malware installs a Trojan that interacts with installed SIMATIC WinCC and SIMATIC Siemens STEP 7 software. Once installed, the Trojan makes queries to any discovered SIMATIC databases. Siemens made a Security Update available for their SIMATIC Siemens software.

Stuxnet appears to have been a well-resourced, long term project (in development since at least June 2009) with very specific targets. There are multiple variants of the malware and they have utilized two different digital signing certificates, which in itself is somewhat unusual. The malware also contains rootkit code for Programmable Logic Controllers (PLCs), though no real details have been provided. However, this is a very disturbing discovery because SCADA software obtains data from and issues commands to PLCs.

Aside from the aforementioned 0-day Microsoft Windows vulnerability, Stuxnet has been observed using three other 0-day vulnerabilities to infect and spread itself. One of the vulnerabilities involves remote code execution—the Print Spooler vulnerability patched in Microsoft's September Security Release (CVE-2010-2729). The other two vulnerabilities are both local elevation of privilege vulnerabilities and Microsoft intends to address these issues in a future release. Stuxnet also exploits an older Microsoft Windows Server Service RPC handling vulnerability (CVE-2008-4250).

We recommend updating Windows systems with the latest software to close the 0-day holes used by this attack. Scan all USB sticks that will be used in the Siemens' environment, since USB sticks are one of the methods of spreading this worm. IBM Products provide signature coverage for the aforementioned vulnerabilities. Multiple Anti-Virus vendors have also added detection to their products and users should ensure their software is up-to-date.

The increased use of networked SCADA systems combined with the ever increasing threat from terrorism and cyberwar is prompting the industry to pay more attention to the security implications of SCADA installations. There are several threats to these systems. From Denial of service (DoS) attacks to the insider threat and data injection to backdoors, SCADA software faces many of the same threats as other enterprise software. The Q2 2010 edition of IBM's Threat Insight report has an excellent article on the threats facing SCADA systems.

'Here You Have' Worm Impacts the Internet

In Q3 2010, a new worm got the attention of news outlets and quickly spread through many corporations. Win32/Visal.b better known as the "here you have" malware is an Internet based worm and spreads via multiple methods. The most predominate method of infection is via email with the subject line of "here you have", "just for you" or "hi".

The malware utilizes the address book within MS Outlook, as well as obtaining contact information from Yahoo! Messenger. Within that email is a generic spoofing attack containing a link to what appears to be a .pdf document, but when looking at the source the .scr extension is revealed. Win32/Visal.b also spreads through local networks by copying itself to drives C: through H: of the target computer and creates a full access share named "updates" on the local computer.

Protection from these types of attacks should largely come from anti-virus and email gateway protection, as this attack utilizes no known vulnerabilities or attacks against protocols or applications. Users should make sure their signature files are up to date.

Intrusion Detection Systems do, however, have some detection of the attack when tuned and utilized properly. It should be stressed that the best defense in this case is user education. Opening attachments that look suspicious, even if they are from known senders is dangerous.

List of Contributors for this paper include:

IBM MSS Intelligence Center
Michelle Alvarez – Team Lead & Cyber Threat Intelligence Analyst
Michael Montecillo – Senior Threat Analyst

IBM X-Force Database Team

References

The Common Platform of Web Application Attacks
IBM X-Force 2010 Mid-Year Trend and Risk Report
http://www-935.ibm.com/services/us/iss/xforce/trendreports/

IBM X-Force 2008 Annual Trend and Risk Report
http://www-935.ibm.com/services/us/iss/xforce/trendreports/

Wordpress Support. "Godaddy Wordpress Blog Hacked."
http://wordpress.org/support/topic/godaddy-wordpress-blog-hacked

GoDaddy Sites Hacked – myblindstudioinfoonline.com and Hilary Kneber
http://blog.sucuri.net/2010/09/godaddy-sites-hacked-myblindstudioinfoonline-com-and-hilary-kneber.html

Joomla Exploits
http://www.joomlaexploit.com

It Isn't Always Cyber
Social Engineers Successfully Gather Info – Dark Reading
http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=226600101

IBM – Consulting Security Services
https://www-935.ibm.com/services/us/index.wss/offerfamily/gts/a1027703

IBM – Physical security services
https://www-935.ibm.com/services/us/index.wss/offerfamily/gts/a1027703

Prolific and Impacting Issues of Q3 2010
ICS-CERT ADVISORY ICSA-10-201-01—USB MALWARE TARGETING SIEMENS CONTROL SOFTWARE
http://www.us-cert.gov/control_systems/pdf/ICSA-10-201-01%20-%20USB%20Malware%20Targeting%20Siemens%20Control%20Software.pdf

IBM Internet Security Systems Protection Alert: Microsoft Windows Shell Could Allow Remote Code Execution
http://www.iss.net/threats/373.html

SIMATIC Security Update available
http://support.automation.siemens.com/WW/llisapi.dll?=en&caller=view&objid=43876783&func=cslib.csinfo

Stuxnet Using Three Additional Zero-Day Vulnerabilities
http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities

W32.Stuxnet
http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99

IBM X-Force Threat Insight Quarterly – Q2 2010 Edition
ftp://public.dhe.ibm.com/common/ssi/ecm/en/wgl03002usen/WGL03002USEN.PDF

'Here You Have' Email
http://isc.sans.edu/diary.html?storyid=9529

*Information in this document concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2010

Please Recycle

WGL03004-USEN-00