

# Microsoft IIS 6.0 Unsupported Version Detection

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | Microsoft IIS 6.0 Unsupported Version Detection |
| Risk Factor: | Critical |
| Synopsis: | An unsupported version of Microsoft IIS is running on the remote Windows host. |
| Description: | According to its self-reported version number, the installation of Microsoft Internet Information Services (IIS) 6.0 on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. |
| Ips: | 200.32.122.120 (tcp/80) 200.32.122.120 (tcp/1024) |
| Solution: | Upgrade to a version of Microsoft IIS that is currently supported. |

# Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities |
| Risk Factor: | Critical |
| Synopsis: | The remote web server is affected by multiple vulnerabilities. |
| Description: | The 'EBJInvokerServlet' and 'JMXInvokerServlet' servlets hosted on the web server on the remote host are accessible to unauthenticated users. The remote host is, therefore, affected by the following vulnerabilities : - A security bypass vulnerability exists due to improper restriction of access to the console and web management interfaces. An unauthenticated, remote attacker can exploit this, via direct requests, to bypass authentication and gain administrative access. (CVE-2007-1036) - A remote code execution vulnerability exists due to the JMXInvokerHAServlet and EJBInvokerHAServlet invoker servlets not properly restricting access to profiles. An unauthenticated, remote attacker can exploit this to bypass authentication and invoke MBean methods, resulting in the execution of arbitrary code. (CVE-2012-0874) - A remote code execution vulnerability exists in the EJBInvokerServlet and JMXInvokerServlet servlets due to the ability to post a marshalled object. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to install arbitrary applications. Note that this issue is known to affect McAfee Web Reporter versions prior to or equal to version 5.2.1 as well as Symantec Workspace Streaming version 7.5.0.493 and possibly earlier. (CVE-2013-4810) |
| Ips: | 200.32.122.76 (tcp/80) |
| Solution: | If using EMC Data Protection Advisor, either upgrade to version 6.x or apply the workaround for 5.x. Otherwise, contact the vendor or remove any affected JBoss servlets. |

# Microsoft Windows Server 2003 Unsupported Installation Detection

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | Microsoft Windows Server 2003 Unsupported Installation Detection |
| Risk Factor: | Critical |
| Synopsis: | The remote operating system is no longer supported. |
| Description: | The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14th, 2015. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities. |
| Ips: | 200.32.122.120 (tcp/0) |
| Solution: | Upgrade to a version of Windows that is currently supported. |

# SSL Version 2 and 3 Protocol Detection

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | SSL Version 2 and 3 Protocol Detection |
| Risk Factor: | High |
| Synopsis: | The remote service encrypts traffic using a protocol with known weaknesses. |
| Description: | The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. |
| Ips: | 200.32.122.115 (tcp/443) |
| Solution: | Consult the application's documentation to disable SSL 2.0 and 3.0.Use TLS 1.1 (with approved cipher suites) or higher instead. |

# JBoss JMX Console Unrestricted Access

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | JBoss JMX Console Unrestricted Access |
| Risk Factor: | High |
| Synopsis: | The remote web server allows unauthenticated access to an administrative Java servlet. |
| Description: | The remote web server appears to be a version of JBoss that allows unauthenticated access to the JMX and/or Web Console servlets used to manage JBoss and its services. A remote attacker can leverage this issue to disclose sensitive information about the affected application or even take control of it. |
| Ips: | 200.32.122.76 (tcp/80) |
| Solution: | Secure or remove access to the JMX and/or Web Console using the advanced installer options. |

# JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE |
| Risk Factor: | High |
| Synopsis: | The remote host is affected by a remote code execution vulnerability. |
| Description: | The JBoss Application Server installed on the remote host is affected by a remote code execution vulnerability. A flaw in the doFilter method of the ReadOnlyAccessFilter class, of the HTTP Invoker service doesn't restrict classes for which it performs deserialization.This allows a remote, unauthenticated attacker to execute arbitrary code via crafted serialized data. To conduct more accurate test and get precise evidence of RCE exploitation please set 'Perform thorough tests (may disrupt your network or impact scan speed)' setting in the Scan Configuration. |
| Ips: | 200.32.122.76 (tcp/80) |
| Solution: | Follow mitigation guidelines provided in the Red Hat Advisory for CVE-2017-12149. |

# Unencrypted Telnet Server

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | Unencrypted Telnet Server |
| Risk Factor: | Medium |
| Synopsis: | The remote Telnet server transmits traffic in cleartext. |
| Description: | The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session. |
| Ips: | 200.32.122.101 (tcp/23) 200.32.122.102 (tcp/23) |
| Solution: | Disable the Telnet service and use SSH instead. |

# Apache Tomcat Default Files

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | Apache Tomcat Default Files |
| Risk Factor: | Medium |
| Synopsis: | The remote web server contains default files. |
| Description: | The default error page, default index page, example JSPs, and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. |
| Ips: | 200.32.122.120 (tcp/8080) |
| Solution: | Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page. |

# SSL Medium Strength Cipher Suites Supported

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | SSL Medium Strength Cipher Suites Supported |
| Risk Factor: | Medium |
| Synopsis: | The remote service supports the use of medium strength SSL ciphers. |
| Description: | The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. |
| Ips: | 200.32.122.115 (tcp/443) |
| Solution: | Reconfigure the affected application if possible to avoid use of medium strength ciphers. |

# SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| Risk Factor: | Medium |
| Synopsis: | It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. |
| Description: | The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. |
| Ips: | 200.32.122.115 (tcp/443) |
| Solution: | Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. |

# SSH Weak Algorithms Supported

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | SSH Weak Algorithms Supported |
| Risk Factor: | Medium |
| Synopsis: | The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all. |
| Description: | Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. |
| Ips: | 200.32.122.102 (tcp/22) |
| Solution: | Contact the vendor or consult product documentation to remove the weak ciphers. |

# Web Server HTTP Header Internal IP Disclosure

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | Web Server HTTP Header Internal IP Disclosure |
| Risk Factor: | Low |
| Synopsis: | This web server leaks a private IP address through its HTTP headers. |
| Description: | This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. There is a known issue with Microsoft IIS 4.0 doing this in its default configuration. This may also affect other web servers, web applications, web proxies, load balancers and through a variety of misconfigurations related to redirection. |
| Ips: | 200.32.122.120 (tcp/80) 200.32.122.120 (tcp/1024) |
| Solution: | None |

# SSH Server CBC Mode Ciphers Enabled

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | SSH Server CBC Mode Ciphers Enabled |
| Risk Factor: | Low |
| Synopsis: | The SSH server is configured to use Cipher Block Chaining. |
| Description: | The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. |
| Ips: | 200.32.122.80 (tcp/22) 200.32.122.102 (tcp/22) |
| Solution: | Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. |

# SSH Weak MAC Algorithms Enabled

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | SSH Weak MAC Algorithms Enabled |
| Risk Factor: | Low |
| Synopsis: | The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms. |
| Description: | The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. |
| Ips: | 200.32.122.80 (tcp/22) 200.32.122.102 (tcp/22) |
| Solution: | Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms. |

# SSL RC4 Cipher Suites Supported (Bar Mitzvah)

## Identification

Identification here

## Vulnerability detection

Detection here

## Exploitation

Exploitation here

## Detailed findings and recommendations

|  |  |
| --- | --- |
| Vulnerability | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| Risk Factor: | Low |
| Synopsis: | The remote service supports the use of the RC4 cipher. |
| Description: | The remote host supports the use of RC4 in one or more cipher suites.The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. |
| Ips: | 200.32.122.115 (tcp/443) |
| Solution: | Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. |