# TABLE OF CONTENTS

**EXECUTIVE OVERVIEW/KEY FINDINGS** .................................................................................................................. 1  
**DISTRIBUTION OF ATTACK SOURCES** ................................................................................................................ 2  
**COMMAND INJECTION ATTACK METRICS** ........................................................................................................ 3  
**ANATOMY OF A COMMAND INJECTION ATTACK** ................................................................................................. 4  
**COMMON OPERATORS** .................................................................................................................................................. 5  
  - *Redirection Operators* .................................................................................................................................................. 5  
  - *Pipes* ........................................................................................................................................................................................ 5  
  - *Inline commands* ................................................................................................................................................................. 5  
  - *Logical Operators* ............................................................................................................................................................... 5  
**Common Injection Patterns & Results** ......................................................................................................................... 6  
**IBM’S COMMAND INJECTION DETECTION ENGINE** ............................................................................................... 6  
**RECOMMENDATIONS/MITIGATION TECHNIQUES** ....................................................................................................... 7  
**IDPS SIGNATURES** ....................................................................................................................................................... 7  
  - *IBM PROVENTIA* ....................................................................................................................................................................... 7  
  - *AKAMAI* .................................................................................................................................................................................. 7  
  - *CHECKPOINT* ......................................................................................................................................................................... 7  
  - *CISCO IDS* ............................................................................................................................................................................... 9  
  - *INTRUSHIELD* .......................................................................................................................................................................... 11  
  - *PALO ALTO* ............................................................................................................................................................................ 12  
  - *SNORT* .................................................................................................................................................................................... 14  
  - *SOURCEFIRE* ....................................................................................................................................................................... 16  
  - *TIPPING POINT* ................................................................................................................................................................. 17  
**REFERENCES** ............................................................................................................................................................... 20  
**CONTRIBUTORS** .......................................................................................................................................................... 20  
**DISCLAIMER** ............................................................................................................................................................... 20
EXECUTIVE OVERVIEW/KEY FINDINGS

As we look across the threat landscape in search of popular attack methods, we find that while SQL Injection ranks high on the list, command injection attacks are increasing in prevalence and continue to be one of the top attack vectors of choice for threat actors. In a previous paper we discussed SQL injection attacks that IBM has been tracking over the past year. It is imperative that we now take a look at command injection as the pattern of abuse is rising and the risk is extreme.

There have been many reports recently on data breaches in enterprise organizations over the past 6 months. Some of these have been accomplished by using Point of Sale malware. There is some debate over the technique used to deploy POS malware. Some security outlets reported there was enough evidence to suggest phishing campaigns were pointed at company executives and were successful. Even thought that could be true in a limited number of cases, the main avenue into corporate databases points to injection tactics which if successful, allows an attacker to issue arbitrary commands within a vulnerable web application environment. This happens when an application passes unsafe user supplied input (forms, cookies, HTTP headers etc.) to a system shell. If the data input is not validated properly an attacker can “inject” additional shell commands and have them executed with the permissions of the vulnerable application. Simply put, this means a critical web server and its entire data backend could be entirely compromised. This is a serious vulnerability.

Command Injection attacks are one of the most common and successful attacks on the internet. This is primarily due to the complexity needed to protect against them. Their large attack surface and numerous entry points create a cornucopia of opportunities for attackers to compromise a system.
According to IBM’s data, the top attacking country YTD is the United States. It is generally believed that American attackers are more aligned with hacktivist groups but there are single entities which also play a large role in this attack type.
COMMAND INJECTION ATTACK METRICS

Command Injection Incidents YTD

Industries Affected

©Copyright IBM Corporation 2014. All rights reserved. IBM and the IBM logo are trademarks or registered trademarks of the IBM Corporation in the United States, other countries or both. Other company, product or service names may be trademarks or service marks of others.
IBM Managed Security Services has escalated over 38,000 command injection attacks across our entire customer base since January 1, 2014 to present. The large spike in July is directly tied to MuBot activity which was covered and discussed in a Threat Research paper published earlier this year. The spikes in Jan and March were largely tied to Perlbot Irc backdoors. The top attacked industries were Financial and Insurance Services. This observation is directly in line with some of the high profile data breaches that have been recently made public.

The MuBot and Perlbot activity are simply focused upon injecting vulnerable Plesk Desk installations and then setting up a persistent IRC connection back to a command and control host with the sole function of performing vulnerability scans for the Heartbleed vulnerability as well as performing Denial of Service attacks against targets provided by the C&C host. It is important to note however that the spike activity was focused upon attempts to utilize the host as a drone and drain bandwidth. This was not the case in many of the other escalations. In those cases known vulnerable web applications were attacked solely to achieve complete control of the target server.

ANATOMY OF A COMMAND INJECTION ATTACK

Once a vulnerability in an application has been found, an attacker will leverage the vulnerability and place a custom shell script on the target server in order to allow further access. In most cases IBM MSS sees dedicated PHP pages that act as a shell pushed to the target server once the vulnerability has been exploited. When shell access is initiated, the attacker can monitor all processes in order to find additional attack vectors. An example target would be a database user connection which allows injection attacks to be performed directly against the database. The attacker could create setuid files with global read privileges. This would allow the attacker full access and control over the database. Applications are considered vulnerable to command injection attacks if user input is expected in a system level command.
COMMON OPERATORS

Usage of the following operators should be fully restricted within the expected data input fields of any web application.

REDIRECTION OPERATORS
Examples: <, >, >

These operators redirect either input or output somewhere else on the server. < will make whatever comes after it standard input. Replacing the filename with < filename will not change the output, but could be used to avoid some filters. > redirects command output, and can be used to modify files on the server, or create new ones altogether. Combined with the cat command, it could easily be used to add unix users to the system, or deface the website. Finally, >> appends text to a file and is not much different from the original output modifier, but again can be used to avoid some simplistic detection schemes.

PIPES
Examples: |

Pipes allow the user to chain multiple commands. It will redirect the output of one command into the next. So you can run unlimited commands by chaining them with multiple pipes, such as cat file1 | grep "string".

INLINE COMMANDS
Examples: ;, $

This is the original example. Putting a semicolon asks the command line to execute everything before the semicolon, then execute everything else as if on a fresh command line.

LOGICAL OPERATORS
Examples: $, &&, ||

These operators perform some logical operation against the data before and after them on the command line.
COMMON INJECTION PATTERNS & RESULTS
Here are the expected results from a number of common injection patterns (appending the below to a given input string, assuming all quotes are correctly paired:

- `shell_command` - executes the command
- $(shell_command) - executes the command
- `| shell_command` - executes the command and returns the output of the command
- `|| shell_command` - executes the command and returns the output of the command
- `; shell_command` - executes the command and returns the output of the command
- `&& shell_command` executes the command and returns the output of the command
- `> target_file` - overwrites the target file with the output of the previous command
- `>> target_file` - appends the target file with the output of the previous command
- `< target_file` - send contents of target_file to the previous command
- `- operator` - Add additional operations to target command

These are some examples of possible command injection vectors. The full width of attack possibilities is highly dependent upon the underlying function calls. For instance, if an underlying function is using a shell program such as awk, more attack possibilities exist.

IBM’S COMMAND INJECTION DETECTION ENGINE
Relying on raw signature events to detect Command Injection is hardly a perfect solution. IBM has developed a very reliable and robust set of rules within its SIEM environment that allow us nearly a 100% accuracy rate in detection. We see new attack strings on a daily basis which we analyze and implement into the rule sets. New strings are captured within a set of active lists and sent to analysts within minutes of their capture. Once the offending strings are confirmed to be malicious, they are then added to the production detection rules. This proactive solution is unique to IBM.

If a Command Injection attack is escalated to you, it is imperative that you take this action seriously and inspect the target server(s) immediately. Since a large majority of the attack strings are purposely meant to exploit an application first, you MUST ensure your patch management solution is robust.
RECOMMENDATIONS/MITIGATION TECHNIQUES

As with SQL Injection, sanitization of expected user input is a key prevention method. Form and URL data need to be validated for invalid characters. A white list of allowed characters should be created to validate user input.

Web applications and their components should be running strict permissions that never allow any operating system command execution.

IDPS SIGNATURES

Where possible, we recommend that customers immediately enable the signatures listed below for blocking and analyzing any events generated by them. In addition, ensure that any related security patches and anti-virus solutions are up-to-date. These signatures may not be enabled by default.

IBM PROVENTIA

Shell_Command_Injection

AKAMAI

Local File Inclusion (and Command Injection) Using '/proc/self/environ'

System Command Injection

System Command Injection (Unix File Leakage)

System Command Injection (Unix)

CHECKPOINT

Autonomy Connected Backup Type 13 Command Injection

Cogent DataHub Web Server GetPermissions.asp Command Injection

EMC AlphaStor Device Manager Command Injection

EMC AlphaStor Device Manager Command Injection - Improved performance

eScan Web Management Console Command Injection

FritzBox Webcm Unauthenticated Command Injection
HP SiteScope SOAP Call runOMAgentCommand Command Injection
HP System Management Home Page Command Injection
ISC DHCP dhclient Network Configuration Script Command Injection
Mail Content Firefox Command Line URL Shell Command Injection
Microsoft Windows File and Directory Name Command Injection (MS12-048)
Multiple Products STARTTLS Plaintext Command Injection
Nagios Remote Plugin Executor Command Injection
Nagios XI Network Monitor Graph Explorer Component Command Injection
Oracle Secure Backup Administration objectname Variable Command Injection
Oracle Secure Backup Administration preauth Variable Command Injection
Oracle Secure Backup Administration property_box.php Command Injection
Oracle Secure Backup Administration selector Variable Command Injection
Oracle Secure Backup Administration Server Command Injection
Oracle Secure Backup Administration Server validate_login Command Injection
Oracle Secure Backup Multiple Command Injections
Oracle Virtual Server Agent Command Injection
PineApp Mail-SeCure conflivelog.pl Command Injection
PineApp Mail-SeCure confpremenu.php Export Log Command Injection
PineApp Mail-SeCure confpremenu.php Install License Command Injection
PineApp Mail-SeCure livelog.html Command Injection
PineApp Mail-SeCure test_li_connection.php Command Injection
Symantec Web Gateway pbcontrol.php Command Injection
VICIdial Manager Send OS Command Injection
CISCO IDS

5473 Java JNLP File Command Injection
5558.0 - Webcart Command Injection
5574.0 - OpenView Network Node Manager Command Injection
5638 PHP Command Injection
5720 Lyris ListManager SQL Command Injection
6004 IOS HTTP Server Iframe Command Injection
6004.0 IOS HTTP Server Iframe Command Injection
6011 - Internet Explorer FTP Command Injection
BigPond Wireless Broadband Gateway Command Injection
Buffalo TeraStation Command Injection Vulnerability
Cisco SRP 500 Series Web Interface Command Injection Vulnerability
Cisco Telepresence Command Injection Vulnerability
Cisco TelePresence Endpoint CGI Command Injection
Cisco TelePresence Recording Server Media Import Command Injection
Cisco Unified Videoconferencing Remote Command Injection
Cisco WSA Authenticated Command Injection
Cisco WSA, ESA, and SMA Authenticated Command Injection
CiscoWorks Common Services Command Injection
D-Link DIR-600 and DIR-300 Remote Command Injection
Hastymail 2.1.1 RC1 Command Injection
HP Linux Printing And Imaging hpssd Command Injection
HP SAN-iQ Remote Command Injection
HP SiteScope SOAP Call runOMAgntCommand Command Injection
Internet Explorer FTP Command Injection
IOS HTTP Server Iframe Command Injection
iPlanet Web Admin Server Command Injection
Java JNLP File Command Injection
Jet Database Engine Shell Command Injection
Linksys Multiple Routers apply.cgi Remote Command Injection
Linksys Router Command Injection Vulnerability
Linksys WAG200G Command Injection Security Vulnerability
Lyris ListManager SQL Command Injection
Measuresoft ScadaPro Command Injection
Microsoft Sharepoint Command Injection Vulnerability
Nagios XI Autodiscovery Command Injection
NetGear DGN1000B Wireless Router OS Command Injection Vulnerability
OpenView Network Node Manager Command Injection
Oracle Secure Backup Administration Server login.php Command Injection
Oracle Secure Backup Login.php Command Injection
PeaZip 2.6.1 Zip Processing Command Injection
PHP Command Injection
PHP Command Injection Via POP3
PineApp Mail-SeCure Command Injection
SAP NetWeaver SOAP Interface Remote Command Injection
Splunk Command Injection
SynCE Command Injection
Webcart Command Injection
ZamFoo Date Parameter Remote Command Injection

Zavio IP Cameras Command Injection Vulnerability

INTRUSHIELD

DCERPC: ARCServe Backup Command Injection Vulnerability

EMC: EMC AlphaStor Device Manager Command Injection

HTTP: Apple Safari for Windows Protocol Handler Command Injection Vulnerability

HTTP: AWStats Shell Command Injection Vulnerability

HTTP: DD-WRT Web Management Interface Remote Arbitrary Shell Command Injection Vulnerability

HTTP: Dolibarr ERP AND CRM OS Command Injection

HTTP: eScan Web Management Console Command Injection

HTTP: GroundWork monarch_scan.cgi OS Command Injection

HTTP: HP SiteScope SOAP Call runOMAgentCommand Command Injection

HTTP: HP System Management Homepage JustGetSNMPQueue Command Injection

HTTP: IBM Lotus Expeditor rcplauncher Command Injection

HTTP: Landesk OS command injection

HTTP: LifeSize Room Command Injection Vulnerabilities

HTTP: Microsoft Windows Shell Command Injection Remote Code Execution

HTTP: Mitel Audio And Web Conferencing Command Injection

HTTP: Nagios Command Injection Vulnerability

HTTP: Nagios XI Network Monitor Graph Explorer Component Command Injection

HTTP: Oracle Secure Backup Administration objectname Variable Command Injection

HTTP: Oracle Secure Backup Administration preauth Variable Command Injection

HTTP: Oracle Secure Backup Administration selector Variable Command Injection

HTTP: Oracle Secure Backup Administration Server Command Injection
HTTP: Oracle Secure Backup Administration Server login.php Command Injection
HTTP: PeaZIP Archived File Name Handling Command Injection Exploit
HTTP: PineApp Mail-SeCure confpremenu.php Export Log Command Injection Vulnerability
HTTP: PineApp Mail-SeCure livelog.html Command Injection Vulnerability
HTTP: PineApp Mail-SeCure test_li_connection.php Command Injection
HTTP: SquirrelMail map_yp_alias Command Injection Exploit
HTTP: Ston3d Player Command Injection Exploit
HTTP: Symantec Web Gateway ipchange.php Command Injection Vulnerability
HTTP: TWiki rev Parameter Shell Command Injection
IRON MOUNTAIN: Connected Backup Opcode 13 Processing Command Injection Remote Code Execution
NETBIOS-SS: Microsoft Windows Shell Command Injection Remote Code Execution
SMTP: Firefox URL Shell Command Injection
SYMANTEC: Symantec AMS Intel Handler Service Command Injection
ZABBIX: Zabbix Agent Command Injection Vulnerability

PALO ALTO

Apache HTTP Server Terminal Escape Sequence in Logs Command Injection Vulnerability
CA ARCserve Backup Engine Command Injection Vulnerability
Courier-IMAP XMAILDIR Shell Command Injection Vulnerability
D-Link UPnP M-SEARCH Command Injection Vulnerability
DD-WRT Web Management Interface Command Injection Vulnerability
DX Studio Player Firefox plug-in Command Injection
EMC AlphaStor Device Manager 0x75 Command Injection Remote Code Execution Vulnerability
Firefox Command Line URL Shell Command Injection
Google Apps mailto URI Command Injection Vulnerability

©Copyright IBM Corporation 2014. All rights reserved. IBM and the IBM logo are trademarks or registered trademarks of the IBM Corporation in the United States, other countries or both. Other company, product or service names may be trademarks or service marks of others.
HastyMail RCI Command Injection Vulnerability
HP System Management Homepage Command Injection Vulnerability
IBM Lotus Notes URL Handler Command Injection Vulnerability
Microsoft Internet Explorer and Mozilla Firefox URI Handler Command Injection Vulnerability
Microsoft SharePoint Command Injection Code Execution Vulnerability
Nagios Statuswml Cgi Command Injection Vulnerability
Openfire Remote Command Injection Vulnerability
Oracle Secure Backup Administration Server login.php Command Injection Vulnerability
Oracle Secure Backup Administration Server validate_login Command Injection Vulnerability
Oracle Secure Backup Authentication Bypass Command Injection Vulnerability
Oracle Secure Backup exec_qr Command Injection Vulnerability
Oracle Secure Backup Server Command Injection
Postfix SMTP Service STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability
SAP MaxDB Remote Command Injection Exploit
SAP NetWeaver HostControl Command Injection Vulnerability
Sinapsi eSolar Light Photovoltaic System Monitor Command Injection Vulnerability
Squirrelmail PGP Plugin Command Injection Vulnerability
Sun Solaris rpc.ypupdated Command Injection Vulnerability
Symantec Web Gateway ipchange.php Command Injection Vulnerability
Symantec Web Gateway pbcontrol Command Injection Vulnerability
TWiki rev Parameter Shell Command Injection Vulnerability
SNORT

- BROWSER-FIREFOX Mozilla Firefox command line URL shell command injection attempt
- BROWSER-IE Microsoft Internet Explorer FTP command injection attempt
- DELETED SCADA Measuresoft ScadaPro remote command injection attempt
- DELETED SERVER-OTHER HP OpenView Network Node Manager freeIPaddrs command injection attempt
- DELETED SERVER-OTHER HP OpenView Network Node Manager cdpnode command injection attempt
- DELETED SERVER-OTHER HP OpenView Network Node Manager connectedNodes command injection attempt
- DELETED WEB-CLIENT PeaZip command injection attempt
- EXPLOIT HP OpenView Network Node Manager freeIPaddrs command injection attempt
- EXPLOIT HP OpenView Network Node Manager cdpnode command injection attempt
- EXPLOIT HP OpenView Network Node Manager connectedNodes command injection attempt
- FILE-MULTIMEDIA Worldweaver DX Studio Player plug-in command injection attempt
- FILE-OTHER PeaZip command injection attempt
- FILE-OTHER Telnet protocol specifier command injection attempt
- INDICATOR-COMPROMISE php-shell failed remote command injection attempt
- INDICATOR-COMPROMISE php-shell remote command injection attempt
- NETBIOS Samba username map script command injection attempt
- OS-OTHER Cisco Nexus OS software command injection attempt
- PROTOCOL-SCADA Sinapsi command injection attempt
- SERVER-MAIL Recipient arbitrary command injection attempt
- SERVER-ORACLE Oracle Endeca Server createDataStore remote command injection attempt
- SERVER-ORACLE Oracle Secure Backup Administration objectname variable command injection attempt
- SERVER-ORACLE Oracle Secure Backup Administration selector variable command injection attempt
- SERVER-OTHER F5 BIG-IP remote command injection attempt
SERVER-OTHER HP Linux Imaging and Printing Project hpssd daemon command injection attempt
SERVER-OTHER HP OpenView Network Node Manager freelPaddrs command injection attempt
SERVER-OTHER HP OpenView Network Node Manger cdmpnode command injection attempt
SERVER-OTHER HP OpenView Network Node Manger connectedNodes command injection attempt
SERVER-OTHER MongoDB nativeHelper.apply method command injection attempt
SERVER-OTHER Oracle VM server agent command injection
SERVER-OTHER RaySharp CCTV derivative command injection attempt
SERVER-OTHER Zabbix Agent net.tcp.listen command injection attempt
SERVER-SAMBA Samba username map script command injection attempt
SERVER-WEBAPP alternate xmlrpc.php command injection attempt
SERVER-WEBAPP Cogent DataHub getpermissions.asp command injection attempt
SERVER-WEBAPP HP OpenView Network Node Manager cdpView.ovpl command injection attempt
SERVER-WEBAPP HP OpenView Network Node Manager connectedNodes.ovpl command injection attempt
SERVER-WEBAPP HP OpenView Network Node Manager freelPaddrs.ovpl command injection attempt
SERVER-WEBAPP iPlanet Webserver command injection attempt
SERVER-WEBAPP Oracle Secure Backup Administration preauth variable command injection attempt
SERVER-WEBAPP PineApp Mail-SeCure test_li_connection.php command injection
SERVER-WEBAPP RaidSonic Multiple Products arbitrary command injection attempt
SERVER-WEBAPP Redmine SCM rev parameter command injection attempt
SERVER-WEBAPP SAP NetWeaver SOAP interface command injection attempt
SERVER-WEBAPP Twiki rdiff rev command injection attempt
SERVER-WEBAPP Twiki view rev command injection attempt
SERVER-WEBAPP Twiki viewfile rev command injection attempt
SERVER-WEBAPP WebCalendar index.php form_readonly login parameter command injection
SERVER-WEBAPP WebCalendar index.php form_single_user_login parameter command injection attempt
SERVER-WEBAPP WebCalendar index.php login parameter command injection attempt
SERVER-WEBAPP xmlrpc.php command injection attempt
SMTP ClamAV recipient command injection attempt
SPECIFIC THREAT Metasploit Framework xmlrpc.php command injection attempt
SPECIFIC-THREATS Firefox command line URL shell command injection attempt
WEB-CLIENT Telnet protocol specifier command injection attempt
WEB-CLIENT Worldweaver DX Studio Player plug-in command injection attempt
WEB-MISC Twiki rdiff rev command injection attempt
WEB-MISC Twiki view rev command injection attempt
WEB-MISC Twiki viewfile rev command injection attempt

SOURCEFIRE

EXPLOIT Oracle VM server agent command injection
ORACLE Oracle Secure Backup Administration selector variable command injection attempt
ORACLE Oracle Secure Backup Administration server property_box.php command injection attempt
Oracle Secure Backup Administration Server login.php Cookies Command Injection attempt
ORACLE Secure Backup common.php variable based command injection attempt
ORACLE Secure Backup exec_qr command injection attempt
ORACLE Secure Backup login.php variable based command injection attempt
ORACLE Secure Backup POST exec_qr command injection attempt
OS-WINDOWS Microsoft Windows search protocol remote command injection attempt
SERVER-ORACLE Oracle Secure Backup Administration server property_box.php command injection attempt
SERVER-ORACLE Oracle Secure Backup exec_qr command injection attempt
SERVER-ORACLE Secure Backup administration server login.php cookies command injection attempt

©Copyright IBM Corporation 2014. All rights reserved. IBM and the IBM logo are trademarks or registered trademarks of the IBM Corporation in the United States, other countries or both. Other company, product or service names may be trademarks or service marks of others.
SERVER-ORACLE Secure Backup common.php variable based command injection attempt
SERVER-ORACLE Secure Backup exec_qr command injection attempt
SERVER-ORACLE Secure Backup login.php variable based command injection attempt
SERVER-ORACLE Secure Backup POST exec_qr command injection attempt
SERVER-OTHER EMC AlphaStor Device Manager command injection attempt
SERVER-OTHER Iron Mountain connected backup opcode 13 processing command injection attempt
SERVER-WEBAPP HP System Management arbitrary command injection attempt
SERVER-WEBAPP Oracle Secure Backup Admin Server command injection attempt
SERVER-WEBAPP Oracle Virtual Server Agent command injection attempt
SERVER-WEBAPP PHP-CGI command injection attempt
SERVER-WEBAPP Secure Backup login.php uname variable based command injection attempt
SERVER-WEBAPP Symantec Web Gateway pbcontrol.php filename parameter command injection attempt
SERVER-WEBAPP Webmin show.cgi arbitrary command injection attempt
SPECIFIC-THREATS alternate xmlrpc.php command injection attempt
SPECIFIC-THREATS Metasploit Framework xmlrpc.php command injection attempt
SPECIFIC-THREATS Secure Backup login.php uname variable based command injection attempt
SPECIFIC-THREATS xmlrpc.php command injection attempt
SQL SAP MaxDB shell command injection attempt
WEB-CLIENT DX Studio Player plug-in command injection attempt
WEB-CLIENT Microsoft Internet Explorer FTP command injection attempt
WEB-MISC Oracle Secure Backup Administration preauth variable command injection attempt
WEB-MISC Oracle Virtual Server Agent command injection attempt

**TIPPING POINT**

10451: HTTP: Oracle Secure Backup Command Injection
10454: HTTP: Oracle Secure Backup Command Injection (ZDI-10-118)

11238: HTTP: Oracle Secure Backup validate_login Command Injection (ZDI-11-238)

11274: HTTP: Oracle VM utl_test_url Command Injection

11305: HTTP: Oracle Java Command Injection Vulnerability (ZDI-11-192)

11309: SMTP: STARTTLS Plaintext Command Injection

11457: DHCP: ISC DHCP dhclient Network Configuration Script Command Injection

11766: HTTP: Oracle Secure Backup validate_login Command Injection (ZDI-09-003)

11839: HTTP: IBM Lotus Notes URL Command Injection Vulnerability (ZDI-12-154)

12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability

12630: HTTP: Symantec Web Gateway pbcontrol.php Command Injection

2792: HTTP: HP Web Jetadmin Command Injection Vulnerability

2792: HTTP: HP Web Jetadmin Remote Command Injection Vulnerability

2793: HTTP: HP Web Jetadmin Command Injection Vulnerability

2793: HTTP: HP Web Jetadmin Remote Command Injection Vulnerability

2813: HTTP: HP Web Jetadmin Remote Command Injection Vulnerability

3534: HTTP: Axis Webcam Command Injection Attack

3572: HTTP: Fusion News Command Injection Attack

3618: HTTP: XML-RPC command injection

3756: FTP: FTP Username Command Injection

3910: HTTP: Wordpress Command Injection

4099: HTTP: Horde Help Viewer PHP Command Injection

4578 HTTP: Horde Help Viewer PHP Command Injection

4578: HTTP: Horde Help Viewer PHP Command Injection

4741: HTTP: TWiki Command Injection
5733: HTTP: SquirrelMail G/PGP Command Injection Attack
6330: HTTP: Coppermine Photo Gallery Command Injection
8581: SMTP: ClamAV Command Injection Exploit
8591: HTTP: DD-WRT Web Management Interface Command Injection Vulnerability
8682: SYMANTEC: Symantec System Center Command Injection (ZDI-09-060)
8744: Oracle: Secure Backup Command Injection
8778: HTTP: Oracle Secure Backup Command Injection (ZDI-09-059, ZDI-10-119, ZDI-10-120)
8836: HTTP: GoogleApps URI Argument Command Injection
9087: SMTP: Mozilla Firefox URL Shell Command Injection
9109: HTTP: TWiki rev Parameter Shell Command Injection
9697: HTTP: Oracle Java Web Start Launch Command Injection
9698: HTTP: Oracle Java Web Start Launch Command Injection
9774: HTTP: Mozilla Products URI Handlers Command Injection
REFERENCES

https://www.owasp.org

https://www.golemtechnologies.com/articles/shell-injection

http://www.iss.net/security_center/reference/vuln/Shell_Command_Injection.htm

CONTRIBUTORS

Nicholas Bradley – IBM MSS Threat Research Practice Lead

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. The data contained herein describing tactics, techniques and procedures is classified Confidential for the consumption of IBM MSS clients only.