Risk Analysis Document

Contents

Aim of the Document

This document shows the existing versions of the applications used by 24online and its vulnerabilities. These applications include – Apache Tomcat, Apache, JDK, and Postgresql.

Applications and Vulnerabilities

1] Apache Tomcat

Version: Apache Tomcat 5.0.28

Security Vulnerabilities

#	CVE ID	Score	Availability	Comments
1	CVE-2013-6357	6.8	Partial	** DISPUTED ** Cross-site request forgery (CSRF) vulnerability in the Manager application in Apache Tomcat 5.5.25 and earlier allows remote attackers to hijack the authentication of administrators for requests that manipulate application deployment via the POST method, as demonstrated by a /manager/html/undeploy?path= URI. NOTE: the vendor disputes the significance of this report, stating that "the Apache Tomcat Security team has not accepted any reports of CSRF attacks against the Manager application ... as they require a reckless system administrator."
2	CVE-2013-4590	4.3	None	Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 allows attackers to obtain "Tomcat internals" information by leveraging the presence of an untrusted web application with a context.xml, web.xml, *.jspx, *.tagx, or *.tld XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.
3	CVE-2013-4322	4.3	Partial	Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 processes chunked transfer coding without properly handling (1) a large total amount of chunked data or (2) whitespace characters in an HTTP header value within a trailer field, which allows remote attackers to cause a denial of service by streaming data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3544.
4	CVE-2013-4286	5.8	None	Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090.
5	CVE-2012-5568	5.0	Partial	Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.
6	CVE-2009-3548	7.5	Partial	The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges.
7	CVE-2008-5519	2.6	None	The JK Connector (aka mod_jk) 1.2.0 through 1.2.26 in Apache Tomcat allows remote attackers to obtain sensitive information via an arbitrary request from an HTTP client, in opportunistic circumstances involving (1) a request from a different client that included a Content-Length header but no POST data or (2) a rapid

				series of requests, related to noncompliance with the AJP protocol's requirements for requests containing Content-Length headers.
8	CVE-2007-5333	5.0	None	Apache Tomcat 6.0.0 through 6.0.14, 5.5.0 through 5.5.25, and 4.1.0 through 4.1.36 does not properly handle (1) double quote (") characters or (2) %5C (encoded backslash) sequences in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks. NOTE: this issue exists because of an incomplete fix for CVE-2007-3385.
9	CVE-2007-3385	4.3	None	Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 does not properly handle the \" character sequence in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks.
10	CVE-2007-3382	4.3	None	Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 treats single quotes ("'") as delimiters in cookies, which might cause sensitive information such as session IDs to be leaked and allow remote attackers to conduct session hijacking attacks.
11	CVE-2007-2450	3.5	None	Multiple cross-site scripting (XSS) vulnerabilities in the (1) Manager and (2) Host Manager web applications in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote authenticated users to inject arbitrary web script or HTML via a parameter name to manager/html/upload, and other unspecified vectors.
12	CVE-2007-2449	4.3	None	Multiple cross-site scripting (XSS) vulnerabilities in certain JSP files in the examples web application in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote attackers to inject arbitrary web script or HTML via the portion of the URI after the ';' character, as demonstrated by a URI containing a "snp/snoop.jsp;" sequence.
13	CVE-2007-1858	2.6	None	The default SSL cipher configuration in Apache Tomcat 4.1.28 through 4.1.31, 5.0.0 through 5.0.30, and 5.5.0 through 5.5.17 uses certain insecure ciphers, including the anonymous cipher, which allows remote attackers to obtain sensitive information or have other, unspecified impacts.
14	CVE-2007-1355	4.3	None	Multiple cross-site scripting (XSS) vulnerabilities in the appdev/sample/web/hello.jsp example application in Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.23, and 6.0.0 through 6.0.10 allow remote attackers to inject arbitrary web script or HTML via the test parameter and unspecified vectors.
15	CVE-2007-0450	5.0	None	Directory traversal vulnerability in Apache HTTP Server and Tomcat 5.x before 5.5.22 and 6.x before 6.0.10, when using certain proxy modules (mod_proxy, mod_rewrite, mod_jk), allows remote attackers to read arbitrary files via a .. (dot dot) sequence with combinations of (1) "/" (slash), (2) "\" (backslash), and (3) URL-encoded backslash (%5C) characters in the URL, which are valid separators in Tomcat but not in Apache.
16	CVE-2006-7196	4.3	None	Cross-site scripting (XSS) vulnerability in the calendar application example in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.31, 5.0.0 through 5.0.30, and 5.5.0 through 5.5.15 allows remote attackers to inject arbitrary web script or HTML via the time parameter to cal2.jsp and possibly unspecified other vectors.

				NOTE: this may be related to CVE-2006-0254.1.
17	CVE-2006-7195	**4.3**	None	Cross-site scripting (XSS) vulnerability in implicit-objects.jsp in Apache Tomcat 5.0.0 through 5.0.30 and 5.5.0 through 5.5.17 allows remote attackers to inject arbitrary web script or HTML via certain header values.
18	CVE-2006-3835	**5.0**	None	Apache Tomcat 5 before 5.5.17 allows remote attackers to list directories via a semicolon (;) preceding a filename with a mapped extension, as demonstrated by URLs ending with /;index.jsp and /;help.do.

2] Apache

Version: Apache Http Server 1.3

Security Vulnerabilities

#	CVE ID	Score	Availability	Comments
1	CVE-2013-2249	7.5	Partial	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.
2	CVE-2012-0883	6.9	Complete	envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
3	CVE-2012-0031	4.6	Partial	scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.
4	CVE-2011-4317	4.3	None	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.
5	CVE-2011-3368	5.0	None	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.
6	CVE-2011-3348	4.3	Partial	The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.
7	CVE-2011-3192	7.8	Complete	The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.
8	CVE-2011-0419	4.3	Partial	Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory

				consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.
9	CVE-2010-0010	6.8	Partial	Integer overflow in the ap_proxy_send_fb function in proxy/proxy_util.c in mod_proxy in the Apache HTTP Server before 1.3.42 on 64-bit platforms allows remote origin servers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a large chunk size that triggers a heap-based buffer overflow.
10	CVE-2009-3555	5.8	Partial	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.
11	CVE-2009-2699	5.0	Partial	The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.
12	CVE-2009-1890	7.1	Complete	The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.
13	CVE-2008-0455	4.3	None	Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.
14	CVE-2008-0005	4.3	None	mod_proxy_ftp in Apache 2.2.x before 2.2.7-dev, 2.0.x before 2.0.62-dev, and 1.3.x before 1.3.40-dev does not define a charset, which allows remote attackers to conduct cross-site scripting (XSS) attacks using UTF-7 encoding.
15	CVE-2007-6750	5.0	Partial	The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.
16	CVE-2006-3918	4.3	None	http_protocol.c in (1) IBM HTTP Server 6.0 before 6.0.2.13 and 6.1 before 6.1.0.1, and (2) Apache HTTP Server 1.3 before 1.3.35, 2.0 before 2.0.58, and 2.2 before 2.2.2, does not sanitize the Expect header from an HTTP request when it is reflected back in an error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated using a Flash SWF file.
17	CVE-2005-3352	4.3	None	Cross-site scripting (XSS) vulnerability in the mod_imap module of Apache httpd before 1.3.35-dev and Apache httpd 2.0.x before

				2.0.56-dev allows remote attackers to inject arbitrary web script or HTML via the Referer when using image maps.
18	CVE-2004-1082	7.5	Partial	mod_digest_apple for Apache 1.3.31 and 1.3.32 on Mac OS X Server does not properly verify the nonce of a client response, which allows remote attackers to replay credentials.
19	CVE-2004-0940	6.9	Complete	Buffer overflow in the get_tag function in mod_include for Apache 1.3.x to 1.3.32 allows local users who can create SSI documents to execute arbitrary code as the apache user via SSI (XSSI) documents that trigger a length calculation error.
20	CVE-2004-0488	7.5	Partial	Stack-based buffer overflow in the ssl_util_uuencode_binary function in ssl_util.c for Apache mod_ssl, when mod_ssl is configured to trust the issuing CA, may allow remote attackers to execute arbitrary code via a client certificate with a long subject DN.
21	CVE-2004-0263	5.0	None	PHP 4.3.4 and earlier in Apache 1.x and 2.x (mod_php) can leak global variables between virtual hosts that are handled by the same Apache child process but have different settings, which could allow remote attackers to obtain sensitive information.
22	CVE-2004-0173	5.0	None	Directory traversal vulnerability in Apache 1.3.29 and earlier, and Apache 2.0.48 and earlier, when running on Cygwin, allows remote attackers to read arbitrary files via a URL containing "..%5C" (dot dot encoded backslash) sequences.
23	CVE-2003-0993	7.5	Partial	mod_access in Apache 1.3 before 1.3.30, when running big-endian 64-bit platforms, does not properly parse Allow/Deny rules using IP addresses without a netmask, which could allow remote attackers to bypass intended access restrictions.
24	CVE-2003-0542	7.2	Complete	Multiple stack-based buffer overflows in (1) mod_alias and (2) mod_rewrite for Apache before 1.3.29 allow attackers to create configuration files to cause a denial of service (crash) or execute arbitrary code via a regular expression with more than 9 captures.
25	CVE-2003-0083	5.0	None	Apache 1.3 before 1.3.25 and Apache 2.0 before version 2.0.46 does not filter terminal escape sequences from its access logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences, a different vulnerability than CVE-2003-0020.
26	CVE-2002-2272	7.8	Complete	Tomcat 4.0 through 4.1.12, using mod_jk 1.2.1 module on Apache 1.3 through 1.3.27, allows remote attackers to cause a denial of service (desynchronized communications) via an HTTP GET request with a Transfer-Encoding chunked field with invalid values.
27	CVE-2002-0843	7.5	Partial	Buffer overflows in the ApacheBench benchmark support program (ab.c) in Apache before 1.3.27, and Apache 2.x before 2.0.43, allow a malicious web server to cause a denial of service and possibly execute arbitrary code via a long response.
28	CVE-2002-0840	6.8	Partial	Cross-site scripting (XSS) vulnerability in the default error page of Apache 2.0 before 2.0.43, and 1.3.x up to 1.3.26, when UseCanonicalName is "Off" and support for wildcard DNS is present, allows remote attackers to execute script as other web page visitors via the Host: header, a different vulnerability than CAN-2002-1157.
29	CVE-2002-0392	7.5	Partial	Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a chunk-encoded HTTP request that causes Apache to use an incorrect size.
30	CVE-2001-1449	7.5	Partial	The default installation of Apache before 1.3.19 on Mandrake Linux

				7.1 through 8.0 and Linux Corporate Server 1.0.1 allows remote attackers to list the directory index of arbitrary web directories.
31	CVE-2001-0042	**5.0**	None	PHP 3.x (PHP3) on Apache 1.3.6 allows remote attackers to read arbitrary files via a modified .. (dot dot) attack containing "%5c" (encoded backslash) sequences.

3] JDK

Version: SUN JDK 1.6.0 Update 18

Security Vulnerabilities

#	CVE ID	Score	Availability	Comments
1	CVE-2010-0886	**10.0**	Complete	Unspecified vulnerability in the Java Deployment Toolkit component in Oracle Java SE and Java for Business JDK and JRE 6 Update 10 through 19 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

4] PostgreSQL

Version: Postgresql 8.0.1

Security Vulnerabilities

#	CVE ID	Score	Availability	Comments
1	CVE-2010-3433	6.0	Partial	The PL/perl and PL/Tcl implementations in PostgreSQL 7.4 before 7.4.30, 8.0 before 8.0.26, 8.1 before 8.1.22, 8.2 before 8.2.18, 8.3 before 8.3.12, 8.4 before 8.4.5, and 9.0 before 9.0.1 do not properly protect script execution by a different SQL user identity within the same session, which allows remote authenticated users to gain privileges via crafted script code in a SECURITY DEFINER function, as demonstrated by (1) redefining standard functions or (2) redefining operators, a different vulnerability than CVE-2010-1168, CVE-2010-1169, CVE-2010-1170, and CVE-2010-1447.
2	CVE-2010-1975	5.5	None	PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, and 8.4 before 8.4.4 does not properly check privileges during certain RESET ALL operations, which allows remote authenticated users to remove arbitrary parameter settings via a (1) ALTER USER or (2) ALTER DATABASE statement.
3	CVE-2010-1447	8.5	Complete	The Safe (aka Safe.pm) module 2.26, and certain earlier versions, for Perl, as used in PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2, allows context-dependent attackers to bypass intended (1) Safe::reval and (2) Safe::rdo access restrictions, and inject and execute arbitrary code, via vectors involving subroutine references and delayed execution.
4	CVE-2010-1170	6.0	Partial	The PL/Tcl implementation in PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 loads Tcl code from the pltcl_modules table regardless of the table's ownership and permissions, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Tcl code by creating this table and inserting a crafted Tcl script.
5	CVE-2010-1169	8.5	Complete	PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl. NOTE: some sources report that this issue is the same as CVE-2010-1447.
6	CVE-2010-0733	3.5	Partial	Integer overflow in src/backend/executor/nodeHash.c in PostgreSQL 8.4.1 and earlier, and 8.5 through 8.5alpha2, allows remote authenticated users to cause a denial of service (daemon crash) via a SELECT statement with many LEFT JOIN clauses, related to certain hashtable size calculations.
7	CVE-2009-4136	6.5	Partial	PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly manage session-local state during execution of an index function by a database superuser, which

				allows remote authenticated users to gain privileges via a table with crafted index functions, as demonstrated by functions that modify (1) search_path or (2) a prepared statement, a related issue to CVE-2007-6600 and CVE-2009-3230.
8	CVE-2009-4034	**5.8**	Partial	PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based PostgreSQL servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended client-hostname restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
9	CVE-2009-3230	**6.5**	Partial	The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, 8.2 before 8.2.14, 8.1 before 8.1.18, 8.0 before 8.0.22, and 7.4 before 7.4.26 does not use the appropriate privileges for the (1) RESET ROLE and (2) RESET SESSION AUTHORIZATION operations, which allows remote authenticated users to gain privileges. NOTE: this is due to an incomplete fix for CVE-2007-6600.
10	CVE-2007-6601	**7.2**	Complete	The DBLink module in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, 7.4 before 7.4.19, and 7.3 before 7.3.21, when local trust or ident authentication is used, allows remote attackers to gain privileges via unspecified vectors. NOTE: this issue exists because of an incomplete fix for CVE-2007-3278.
11	CVE-2007-6600	**6.5**	Partial	PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, 7.4 before 7.4.19, and 7.3 before 7.3.21 uses superuser privileges instead of table owner privileges for (1) VACUUM and (2) ANALYZE operations within index functions, and supports (3) SET ROLE and (4) SET SESSION AUTHORIZATION within index functions, which allows remote authenticated users to gain privileges.
12	CVE-2007-6067	**6.8**	Complete	Algorithmic complexity vulnerability in the regular expression parser in TCL before 8.4.17, as used in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, and 7.4 before 7.4.19, allows remote authenticated users to cause a denial of service (memory consumption) via a crafted "complex" regular expression with doubly-nested states.
13	CVE-2007-4772	**4.0**	Partial	The regular expression parser in TCL before 8.4.17, as used in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, and 7.4 before 7.4.19, allows context-dependent attackers to cause a denial of service (infinite loop) via a crafted regular expression.
14	CVE-2007-4769	**6.8**	Complete	The regular expression parser in TCL before 8.4.17, as used in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, and 7.4 before 7.4.19, allows remote authenticated users to cause a denial of service (backend crash) via an out-of-bounds backref number.
15	CVE-2007-0556	**6.6**	Complete	The query planner in PostgreSQL before 8.0.11, 8.1 before 8.1.7, and 8.2 before 8.2.2 does not verify that a table is compatible with a "previously made query plan," which allows remote authenticated users to cause a denial of service (server crash) and possibly access database content via an "ALTER COLUMN TYPE" SQL statement, which can be leveraged to read arbitrary memory from the server.
16	CVE-2006-5541	**4.0**	Partial	backend/parser/parse_coerce.c in PostgreSQL 7.4.1 through 7.4.14, 8.0.x before 8.0.9, and 8.1.x before 8.1.5 allows remote

				authenticated users to cause a denial of service (daemon crash) via a coercion of an unknown element to ANYARRAY.
17	CVE-2006-5540	4.0	Partial	backend/parser/analyze.c in PostgreSQL 8.1.x before 8.1.5 allows remote authenticated users to cause a denial of service (daemon crash) via certain aggregate functions in an UPDATE statement, which are not properly handled during a "MIN/MAX index optimization."
18	CVE-2006-2314	7.5	Partial	PostgreSQL 8.1.x before 8.1.4, 8.0.x before 8.0.8, 7.4.x before 7.4.13, 7.3.x before 7.3.15, and earlier versions allows context-dependent attackers to bypass SQL injection protection methods in applications that use multibyte encodings that allow the "\" (backslash) byte 0x5c to be the trailing byte of a multibyte character, such as SJIS, BIG5, GBK, GB18030, and UHC, which cannot be handled correctly by a client that does not understand multibyte encodings, aka a second variant of "Encoding-Based SQL Injection." NOTE: it could be argued that this is a class of issue related to interaction errors between the client and PostgreSQL, but a CVE has been assigned since PostgreSQL is treating this as a preventative measure against this class of problem.
19	CVE-2006-2313	7.5	Partial	PostgreSQL 8.1.x before 8.1.4, 8.0.x before 8.0.8, 7.4.x before 7.4.13, 7.3.x before 7.3.15, and earlier versions allows context-dependent attackers to bypass SQL injection protection methods in applications via invalid encodings of multibyte characters, aka one variant of "Encoding-Based SQL Injection."
20	CVE-2006-0678	1.5	Partial	PostgreSQL 7.3.x before 7.3.14, 7.4.x before 7.4.12, 8.0.x before 8.0.7, and 8.1.x before 8.1.3, when compiled with Asserts enabled, allows local users to cause a denial of service (server crash) via a crafted SET SESSION AUTHORIZATION command, a different vulnerability than CVE-2006-0553.
21	CVE-2006-0105	5.0	Partial	PostgreSQL 8.0.x before 8.0.6 and 8.1.x before 8.1.2, when running on Windows, allows remote attackers to cause a denial of service (postmaster exit and no new connections) via a large number of simultaneous connection requests.
22	CVE-2005-1410	2.1	Partial	The tsearch2 module in PostgreSQL 7.4 through 8.0.x declares the (1) dex_init, (2) snb_en_init, (3) snb_ru_init, (4) spell_init, and (5) syn_init functions as "internal" even when they do not take an internal argument, which allows attackers to cause a denial of service (application crash) and possibly have other impacts via SQL commands that call other functions that accept internal arguments.
23	CVE-2005-1409	7.5	Partial	PostgreSQL 7.3.x through 8.0.x gives public EXECUTE access to certain character conversion functions, which allows unprivileged users to call those functions with malicious values, with unknown impact, aka the "Character conversion vulnerability."
24	CVE-2005-0247	6.5	Partial	Multiple buffer overflows in gram.y for PostgreSQL 8.0.1 and earlier may allow attackers to execute arbitrary code via (1) a large number of variables in a SQL statement being handled by the read_sql_construct function, (2) a large number of INTO variables in a SELECT statement being handled by the make_select_stmt function, (3) a large number of arbitrary variables in a SELECT statement being handled by the make_select_stmt function, and (4) a large number of INTO variables in a FETCH statement being handled by the make_fetch_stmt function, a different set of vulnerabilities than CVE-2005-0245.

Corporate
904, Silicon Tower, Behind Pariseema Building, Off C.G.Road, Nr. Lal Bungalow, Ahmedabad 380 006, INDIA.
Tel: +91-79-66065606 Fax: +91-79-26407640 Email: sales@elitecore.com

Corporate
904, Silicon Tower,
Behind Pariseema Building,
Off C.G.Road, Nr. Lal Bungalow,
Ahmedabad 380 006, INDIA.
Tel: +91-79-66065606
Fax: +91-79-26407640
Email: sales@elitecore.com
sales@cyberoam.com

Mumbai
S1 The Link, 2nd Floor,
New Link Road,
Near Audi Showroom, Andheri (w),
Mumbai 400058, INDIA.
Tel: +91-22-61435100
Fax: +91-22-61435151

Delhi
606, Mahatta Tower,
B Block, Community Centre,
Janakpuri,
New Delhi - 110058, INDIA.
Tel: +91-11-41589761/62
Fax: +91-11-41589760

South Africa
Elitecore Technologies
Block 15, Woodmead Office Park
140 Western Service Road
Woodmead, 2157
Johannesburg, South Africa
Tel: +27-83-301-6055
Fax: +27-86-5181-432

U.S.A
Elitecore Technologies PLC
137½ 10, Shalks Crossing
Road,
Suite 501-329,
Plainsboro, NJ 08536
USA
Tel: +1-781-460-2080
Fax: +1-201-735-5888

Bangalore
'A' Block, 2nd Floor, 'Malik
Embassy'
No.9, Union Street,
Off Infantry Road
Bangalore - 560001, INDIA.
Tel: +91-80-40869000
Fax: +91-80-40869001

Dubai
Office 423, 3rd East Wing
Building,
4th Floor
Dubai Airport Free Zone
P.O. Box 54620
Dubai, U.A.E.
Mobile : +971-50-5512789