Inspector ScanDAll Reports

CVE-2011-0762

The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.

CVE-2014-2685

The GenericConsumer class in the Consumer component in ZendOpenId before 2.0.2 and the Zend_OpenId_Consumer class in Zend Framework 1 before 1.12.4 violate the OpenID 2.0 protocol by ensuring only that at least one field is signed, which allows remote attackers to bypass authentication by leveraging an assertion from an OpenID provider.

CVE-2017-9482

The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote attackers to obtain root access to the Network Processor (NP) Linux system by enabling a TELNET daemon (through CVE-2017-9479 exploitation) and then establishing a TELNET session.

CVE-2011-1720

The SMTP server in Postfix before 2.5.13, 2.6.x before 2.6.10, 2.7.x before 2.7.4, and 2.8.x before 2.8.3, when certain Cyrus SASL authentication methods are enabled, does not create a new server handle after client authentication fails, which allows remote attackers to cause a denial of service (heap memory corruption and daemon crash) or possibly execute arbitrary code via an invalid AUTH command with one method followed by an AUTH command with a different method.

CVE-2008-0122

Off-by-one error in the inet_network function in libbind in ISC BIND 9.4.2 and earlier, as used in libc in FreeBSD 6.2 through 7.0-PRERELEASE, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted input that triggers memory corruption.

CVE-2014-0032

The get_resource function in repos.c in the mod_dav_svn module in Apache Subversion before 1.7.15 and 1.8.x before 1.8.6, when SVNListParentPath is enabled, allows remote attackers to cause a denial of service (crash) via vectors related to the server root and request methods other than GET, as demonstrated by the “svn ls http://svn.example.com” command.

CVE-2016-9772

OpenAFS 1.6.19 and earlier allows remote attackers to obtain sensitive directory information via vectors involving the (1) client cache partition, (2) fileserver vice partition, or (3) certain RPC responses.

CVE-2016-2119

libcli/smb/smbXcli_base.c in Samba 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5 allows man-in-the-middle attackers to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers, via the (1) SMB2_SESSION_FLAG_IS_GUEST or (2) SMB2_SESSION_FLAG_IS_NULL flag.

CVE-2016-2119

libcli/smb/smbXcli_base.c in Samba 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5 allows man-in-the-middle attackers to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers, via the (1) SMB2_SESSION_FLAG_IS_GUEST or (2) SMB2_SESSION_FLAG_IS_NULL flag.

CVE-2006-0769

Unspecified vulnerability in in.rexecd in Solaris 10 allows local users to gain privileges on Kerberos systems via unknown attack vectors.

CVE-2011-0419

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.

CVE-2008-5659

The gnu.java.security.util.PRNG class in GNU Classpath 0.97.2 and earlier uses a predictable seed based on the system time, which makes it easier for context-dependent attackers to conduct brute force attacks against cryptographic routines that use this class for randomness, as demonstrated against DSA private keys.

CVE-2018-7738

In util-linux before 2.32-rc1, bash-completion/umount allows local users to gain privileges by embedding shell commands in a mountpoint name, which is mishandled during a umount command (within Bash) by a different user, as demonstrated by logging in as root and entering umount followed by a tab character for autocompletion.

CVE-2018-7203

Cross-site scripting (XSS) vulnerability in Twonky Server 7.0.11 through 8.5 allows remote attackers to inject arbitrary web script or HTML via the friendly-name parameter to rpc/set_all.

CVE-2009-0543

ProFTPD Server 1.3.1, with NLS support enabled, allows remote attackers to bypass SQL injection protection mechanisms via invalid, encoded multibyte characters, which are not properly handled in (1) mod_sql_mysql and (2) mod_sql_postgres.

CVE-2018-7251

An issue was discovered in config/error.php in Anchor 0.12.3. The error log is exposed at an errors.log URI, and contains MySQL credentials if a MySQL error (such as "Too many connections") has occurred.

CVE-2017-7486

PostgreSQL versions 8.4 - 9.6 are vulnerable to information leak in pg_user_mappings view which discloses foreign server passwords to any user having USAGE privilege on the associated foreign server.

CVE-2014-7815

The set_pixel_format function in ui/vnc.c in QEMU allows remote attackers to cause a denial of service (crash) via a small bytes_per_pixel value.

CVE-2017-7084

An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "Application Firewall" component. It allows remote attackers to bypass intended settings in opportunistic circumstances by leveraging incorrect handling of a denied setting after an upgrade.

CVE-2017-13649

UnrealIRCd 4.0.13 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command. NOTE: the vendor indicates that there is no common or recommended scenario in which a root script would execute this kill command.

CVE-2008-5519

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.

CVE-2017-6056

It was discovered that a programming error in the processing of HTTPS requests in the Apache Tomcat servlet and JSP engine may result in denial of service via an infinite loop. The denial of service is easily achievable as a consequence of backporting a CVE-2016-6816 fix but not backporting the fix for Tomcat bug 57544. Distributions affected by this backporting issue include Debian (before 7.0.56-3+deb8u8 and 8.0.14-1+deb8u7 in jessie) and Ubuntu.

==========

Solution

Firstly, most of attacks occur because of using the old versions of the services. You must try to update your applications as frequently as possible. Also, you can and should disable unneeded services on your systems. Like reducing the number of entry points in your house, the more enrty points you eliminate the fewer places an intruder can break in.

[This work is made by A. Murzaeva, C. Yilmaz and Z. Mutlu]