

TLSA-2006-0024 – multi

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-05/msg00099.html>

- *From:* Trustix Security Advisor <tsl@xxxxxxxxxxx>
 - *Date:* Fri, 5 May 2006 15:28:47 +0200
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Trustix Secure Linux Security Advisory #2006-0024

Package names: clamav, cyrus-sasl, kernel, libtiff, rsync, xorg-x11

Summary: Multiple vulnerabilities

Date: 2006-05-05

Affected versions: Trustix Secure Linux 2.2

Trustix Secure Linux 3.0

Trustix Operating System – Enterprise Server 2

Package description:

clamav

Clam AntiVirus is a GPL anti-virus toolkit for UNIX. The main purpose of this software is the integration with mail servers (attachment scanning).

The package provides a flexible and scalable multi-threaded daemon, a command line scanner, and a tool for automatic updating via Internet.

The programs are based on a shared library distributed with package, which you can use with your own software.

cyrus-sasl

The cyrus-sasl package contains the Cyrus implementation of SASL.

SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols.

kernel

The kernel package contains the Linux kernel (vmlinuz), the core of your Trustix Secure Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation,

device input and output, etc.

libtiff

The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the

.tif extension and they are often quite large.

rsync

Rsync uses a quick and reliable algorithm to very quickly bring remote and host files into sync. Rsync is fast because it just sends the differences in the files over the network (instead of sending the complete files). Rsync is often used as a very powerful mirroring process or just as a more capable replacement for the rcp command. A technical report which describes the rsync algorithm is included in this package.

xorg-x11

X.org X11 is an open source implementation of the X Window System. It provides the basic low level functionality which full fledged graphical user interfaces (GUIs) such as GNOME and KDE are designed upon.

Problem description:

clamav < TSL 3.0 > < TSL 2.2 >

- New Upstream.
- SECURITY Fix: A vulnerability has been reported in ClamAV caused due to a boundary error within the HTTP client in the Freshclam command line utility. This can be exploited to cause a stack-based buffer overflow when the HTTP headers received from a web server exceeds 8KB.

The Common Vulnerabilities and Exposures project has assigned the name CVE-2006-1989 this issue.

cyrus-sasl < TSL 3.0 > < TSL 2.2 > < TSEL 2 >

- SECURITY Fix: Mu Security has reported a vulnerability in Cyrus SASL library, which can be exploited by malicious people to cause a DoS. The vulnerability is caused due to an unspecified error during DIGEST-MD5 negotiation.

The Common Vulnerabilities and Exposures project has assigned the name CVE-2006-1721 this issue.

kernel < TSL 3.0 >

- New Upstream.
- SECURITY Fix: A vulnerability has been reported in Linux Kernel, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to missing checks on SCTP chunk sizes in the SCTP-netfilter code and may result in an infinite loop exhausting system resources.
- Directory traversal vulnerability in CIFS which allows local users to escape chroot restrictions for an SMB-mounted filesystem via "..\\\" sequences.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CVE-2006-1527 and CVE-2006-1863 to these issues.

TLSA-2006-0024 – multi

libtiff < TSL 3.0 > < TSL 2.2 > < TSEL 2 >

- SECURITY Fix: Tavis Ormandy has reported some vulnerabilities in LibTIFF, which can be exploited by malicious people to cause a DoS and potentially to compromise a user's system.
- Several unspecified errors in the "TIFFFetchAnyArray()" function and in the cleanup functions can be exploited to crash an application linked against LibTIFF when a specially crafted TIFF image is processed.
- Integer overflow in the TIFFFetchData function in tif_dirread.c allows context-dependent attackers to cause a denial of service and possibly execute arbitrary code via a crafted TIFF image.
- A double free error in tif_jpeg.c within the setfield/getfield methods in the cleanup functions can be exploited to crash an application linked against LibTIFF and may allow arbitrary code execution when a specially crafted TIFF image is processed.
- The TIFFToRGB function in libtiff allows remote attackers to cause a denial of service (crash) via a crafted TIFF image with Yr/Yg/Yb values that exceed the YCR/YCG/YCB values, which triggers an out-of-bounds read.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CVE-2006-2024, CVE-2006-2025, CVE-2006-2026 and CVE-2006-2120 these issues.

rsync < TSL 3.0 > < TSL 2.2 > < TSEL 2 >

- New Upstream.
- SECURITY Fix: A vulnerability has been reported in rsync caused due to an integer overflow error in the "receive_xattr()" function within the xattrs.diff patch. This can be exploited to cause a buffer overflow and may allow arbitrary code execution via specially crafted extended attributes.

The Common Vulnerabilities and Exposures project has assigned the name CVE-2006-2083 this issue.

xorg-x11 < TSL 3.0 >

- SECURITY Fix: A buffer overflow in the XRender extension allows any X.Org user to execute arbitrary code with elevated privileges. A typo causes the code to mis-compute the size of memory allocations in the XRenderCompositeTriStrip and XRenderCompositeTriFan requests.

The Common Vulnerabilities and Exposures project has assigned the name CVE-2006-1526 this issue.

Action:

We recommend that all systems with this package installed be upgraded. Please note that if you do not need the functionality provided by this package, you may want to remove it from your system.

Location:

All Trustix Secure Linux updates are available from
<URI:<http://http.trustix.org/pub/trustix/updates/>>

<URI:<ftp://ftp.trustix.org/pub/trustix/updates/>>

About Trustix Secure Linux:

Trustix Secure Linux is a small Linux distribution for servers. With focus on security and stability, the system is painlessly kept safe and up to date from day one using swup, the automated software updater.

Automatic updates:

Users of the SWUP tool can enjoy having updates automatically installed using 'swup --upgrade'.

Questions?

Check out our mailing lists:

<URI:<http://www.trustix.org/support/>>

Verification:

This advisory along with all Trustix packages are signed with the TSL sign key.

This key is available from:

<URI:<http://www.trustix.org/TSL-SIGN-KEY>>

The advisory itself is available from the errata pages at

<URI:<http://www.trustix.org/errata/trustix-2.2/>> and

<URI:<http://www.trustix.org/errata/trustix-3.0/>>

or directly at

<URI:<http://www.trustix.org/errata/2006/0024/>>

MD5sums of the packages:

8f9fd0f2b05c574bf2f42841eb84bb05 3.0/rpms/clamav-0.88.2-1tr.i586.rpm
f018f1d168962aca4312c6fe17d2b133 3.0/rpms/clamav-devel-0.88.2-1tr.i586.rpm
975e9e4a862f0518d892aded818d870d 3.0/rpms/cyrus-sasl-2.1.20-15tr.i586.rpm
10484d9cfc683b883bdbb5b20a02681d 3.0/rpms/cyrus-sasl-devel-2.1.20-15tr.i586.rpm
ed57cdfd3c9b21d3ee244d4825a61fc0 3.0/rpms/cyrus-sasl-md5-2.1.20-15tr.i586.rpm
bb6bd68737f8e2fa31489b88ca6163bd 3.0/rpms/cyrus-sasl-otp-2.1.20-15tr.i586.rpm
393f554144e646017016f813bbcaaf06 3.0/rpms/cyrus-sasl-plain-2.1.20-15tr.i586.rpm
6422bf4c3007cad3a35e5c6eeeb29889 3.0/rpms/cyrus-sasl-sql-2.1.20-15tr.i586.rpm
29f1fc6b4dd34e6efc0314b38874c1a4 3.0/rpms/cyrus-sasl-utils-2.1.20-15tr.i586.rpm
fc0f1ce0337ef359fddce5c48610574c 3.0/rpms/kernel-2.6.16.13-1tr.i586.rpm
128a17a5ee280460228ff973d044c2d6 3.0/rpms/kernel-doc-2.6.16.13-1tr.i586.rpm
40b294479e91c9a35e68ce9e2b1e300d 3.0/rpms/kernel-headers-2.6.16.13-1tr.i586.rpm
a82b83e463fab1f07f3c11fa56e86055 3.0/rpms/kernel-smp-2.6.16.13-1tr.i586.rpm
a78d4799876d39e0ce5b3cba16454f69 3.0/rpms/kernel-smp-headers-2.6.16.13-1tr.i586.rpm
9eb0e5c0c63288246a4816d79b8c7d55 3.0/rpms/kernel-source-2.6.16.13-1tr.i586.rpm
cdde0ae2d48aa534dbaf20c67eb2eca6 3.0/rpms/kernel-utils-2.6.16.13-1tr.i586.rpm
8dbc912920dda86e2f9d623f6f88c5af 3.0/rpms/libtiff-3.7.3-2tr.i586.rpm

8e9a0e6917f9529c3720a3dcb101fe2c 3.0/rpms/libtiff-devel-3.7.3-2tr.i586.rpm
 abb3f9444f533b610873eeb22100f2f3 3.0/rpms/libtiff-docs-3.7.3-2tr.i586.rpm
 fc3d971697486d9cba85f81e617120cd 3.0/rpms/rsync-2.6.8-1tr.i586.rpm
 fc722769b558d7f4d22e00bb929a4f5b 3.0/rpms/rsync-server-2.6.8-1tr.i586.rpm
 c48de68cf51aaa7e97b3bc7727bb83cc 3.0/rpms/xorg-x11-6.8.2-11tr.i586.rpm
 5d8bff276211197de40e04f19046d00f 3.0/rpms/xorg-x11-devel-6.8.2-11tr.i586.rpm
 3a346ecc4f058d0c5fd1936b4b8c7826 3.0/rpms/xorg-x11-doc-6.8.2-11tr.i586.rpm
 038487208366b11b1064feb8af2700ed 3.0/rpms/xorg-x11-fonts-100dpi-6.8.2-11tr.i586.rpm
 f5768dab5cb3017630804184e150435e 3.0/rpms/xorg-x11-fonts-6.8.2-11tr.i586.rpm
 d873cb5592008211ec7047e1c32ee857 3.0/rpms/xorg-x11-fonts-75dpi-6.8.2-11tr.i586.rpm
 87f9a7b00656d1ee91df99a09eb96791 3.0/rpms/xorg-x11-fonts-cid-6.8.2-11tr.i586.rpm
 5781bca9e84dc2339e83610254a456c3 3.0/rpms/xorg-x11-fonts-cyrillic-6.8.2-11tr.i586.rpm
 58d6470e0fb229c87d2073dc15c21726 3.0/rpms/xorg-x11-fonts-otf-6.8.2-11tr.i586.rpm
 ab6be3f5dbc41b1ba945188aaf676ba5 3.0/rpms/xorg-x11-fonts-speedo-6.8.2-11tr.i586.rpm
 6f87b1cf6e840b10b8710427722db3d2 3.0/rpms/xorg-x11-fonts-ttf-6.8.2-11tr.i586.rpm
 cee4c07f06da1ecf68a802d0a4d68bea 3.0/rpms/xorg-x11-fonts-type1-6.8.2-11tr.i586.rpm
 10944512010fbd199a864d00c3383615 3.0/rpms/xorg-x11-libs-6.8.2-11tr.i586.rpm
 9ea9d3e411b25eee89af0d65ccdf0eb5 3.0/rpms/xorg-x11-sdk-6.8.2-11tr.i586.rpm

4ce128f09ab5a6aebc814a4a8389cd51 2.2/rpms/clamav-0.88.2-1tr.i586.rpm
 7c29e1c6eab44f4380af89384e18ce67 2.2/rpms/clamav-devel-0.88.2-1tr.i586.rpm
 251875bae4da0c8812f392645454afeb 2.2/rpms/cyrus-sasl-2.1.20-7tr.i586.rpm
 94398d80360b5166a71adc02a700846b 2.2/rpms/cyrus-sasl-devel-2.1.20-7tr.i586.rpm
 0c6fe11ab11c80df5725a738b8500eb2 2.2/rpms/cyrus-sasl-md5-2.1.20-7tr.i586.rpm
 058d6dc0df428df3c1453df769428e9c 2.2/rpms/cyrus-sasl-otp-2.1.20-7tr.i586.rpm
 30d784607cb89d03aaaa860e2ded2902 2.2/rpms/cyrus-sasl-plain-2.1.20-7tr.i586.rpm
 0f794362b7795c05d75f2847bcf1245b 2.2/rpms/cyrus-sasl-sql-2.1.20-7tr.i586.rpm
 0d064a6ff40a2ae53cd93bfd14dbe10c 2.2/rpms/cyrus-sasl-utils-2.1.20-7tr.i586.rpm
 21f4458df3cc75524d89c0ca050d6860 2.2/rpms/libtiff-3.7.3-2tr.i586.rpm
 cb29f7ab911871682000de6316b8ee01 2.2/rpms/libtiff-devel-3.7.3-2tr.i586.rpm
 c2f1d749f54379f1a60202eb7e71e79e 2.2/rpms/rsync-2.6.8-1tr.i586.rpm
 a2ed791cd851db257914372034f448be 2.2/rpms/rsync-server-2.6.8-1tr.i586.rpm

Trustix Security Team

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.2.2 (GNU/Linux)

iD8DBQFEW0Yri8CEzsK9IksRAgPAAKcvVkyOxN7EDyiMwjWAB/s6FrI2MACgr/vB
 xdnR9fI9i96M0vFsTxyXRuY=
 =Cl8X

-----END PGP SIGNATURE-----