

[CERT-intexxia] libgtop_daemon Remote Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-11/0220.html>

From: Benoît Roussel (benoit.roussel@intexxia.com)

Date: 11/27/01

Message-ID: <051a01c17712\$38812930\$403e010a@lab.intexxia.com>

From: Benoît Roussel <benoit.roussel@intexxia.com>

To: "bugtraq" <bugtraq@securityfocus.com>

Subject: [CERT-intexxia] libgtop_daemon Remote Format String Vulnerability

Date: Tue, 27 Nov 2001 08:07:48 +0100

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

Hash: SHA1

SECURITY ADVISORY INTEXXIA(c)

27 11 2001 ID #1048-261101

TITLE : libgtop_daemon Remote Format String Vulnerability

CREDITS : Guillaume Pelat / INTEXXIA

SYSTEM AFFECTED

=====

libgtop_daemon <= 1.0.12

DESCRIPTION

=====

The Laboratory intexxia found a remote exploitable format string vulnerability in libgtop_daemon which could cause privilege escalation on a remote system.

DETAILS

=====

libgtop_daemon is a GNOME daemon used to monitor process running on a remote system.

SecurityFocus Bugtraq: [CERT-intexxia] libgtop_daemon Remote Fo

The Laboratory intexxia just found a remote format string vulnerability in this daemon. The 2 functions named `syslog_message()` and `syslog_io_message()` are called with a format string which is initialized by the client.

By sending a specially crafted format string to the server, it is possible for a remote attacker to execute arbitrary code on the remote system with the daemon permissions. This vulnerability could cause privilege escalation.

The `permitted()` function, that verifies if the client trying to connect is authorized to, is concerned by this flaw.

The `libgtop_daemon` daemon is launched with 'nobody' permissions by default. Complete exploitation of this vulnerability will permit an attacker to execute code with the 'nobody' permissions. But this flaw could be used to compromise the local system by exploiting other local vulnerabilities.

PROOF OF CONCEPT

=====

Here is a proof of concept to show where the problem occurs :

Client side :

```
~ % telnet 127.0.0.1 42800
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
%p%p
Connection closed by foreign host.
~ % telnet 127.0.0.1 42800
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
%n%n
Connection closed by foreign host.
```

Server side :

```
~/# libgtop_daemon -f
' from clientn[3877]: Invalid authentication protocol
'0xbffff46c0x804b2ae
libgtop-daemon[3877]: Refused connection from 127.0.0.1.
Segmentation fault
```

WORKAROUND

=====

SecurityFocus Bugtraq: [CERT-intexxia] libgtop_daemon Remote Fo

Although there is an official solution, here is the way to patch the sources to resolve this problem. The file 'src/daemon/gnuserc.c' must be modified :

In function syslog_message(), replace :

```
syslog (priority, buffer);  
by :  
syslog (priority, "%s", buffer);
```

And in function syslog_io_message(), replace :

```
syslog (priority, buffer2);  
by :  
syslog (priority, "%s", buffer2);
```

The Laboratory intexxia developed the following patch to correct this vulnerability. However, the simplest and probably the best way to resolve this issue is to install the new version at the above link in the solution section :

```
diff -dru libgtop-1.0.12/src/daemon/gnuserc.c  
libgtop-1.0.12-patched/src/daemon/gnuserc.c  
--- libgtop-1.0.12/src/daemon/gnuserc.c Mon Nov 26 13:48:14 2001  
+++ libgtop-1.0.12-patched/src/daemon/gnuserc.c Mon Nov 26 13:49:26 2001  
@@ -93,7 +93,7 @@  
    vsnprintf (buffer, BUFSIZ-1, format, ap);  
    va_end (ap);  
  
- syslog (priority, buffer);  
+ syslog (priority, "%s", buffer);  
}  
  
void  
@@ -108,7 +108,7 @@  
    va_end (ap);  
  
    snprintf (buffer2, BUFSIZ-1, "%s: %s", buffer, strerror (errno));  
- syslog (priority, buffer2);  
+ syslog (priority, "%s", buffer2);  
}  
  
/*
```

SOLUTION

=====

There is an official solution now. libgtop_daemon release 1.0.13 has been made to correct this issue. Here is a link where you can download it :

SecurityFocus Bugtraq: [CERT-intexxia] libgtop_daemon Remote Fo

<http://ftp.gnome.org/pub/GNOME/stable/sources/libgtop/libgtop-1.0.13.tar.gz>

VENDOR STATUS

=====

26-11-2001 : This bulletin was sent to the libgtop_daemon
developpment team.

27-11-2001 : The libgtop_daemon developpement team released a
new version including the patch for this issue.

DISCLAIMER

=====

intexxia provides these informations as a public service and "as
is". Intexxia will not be held accountable for any damage or distress
caused by the proper or improper usage of these materials.

DIFFUSION CRITERIA

=====

(c) intexxia 2001. This document is property of intexxia. Feel
free to use and distribute this material as long as credit is given to
intexxia and the author.

CONTACT

=====

CERT intexxia cert@intexxia.com

INTEXXIA <http://www.intexxia.com>

171, av. Georges Clemenceau Standard : +33 1 55 69 49 10

92024 Nanterre Cedex – France Fax : +33 1 55 69 78 80

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

Version: PGPfreeware 7.0.3 for non-commercial use <<http://www.pgp.com>>

iQA/AwUBPAM7wU2N8BNyNDXLEQLdpQCg1Vi/4vbZQdRjj/1ymF3z1+umSqcAoLg4

FBeGXpWddc3WB6nKK5KMxnC9

=pmZw

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

- *Previous message:* [Klaxon: "Anonymiser.com might reveal your IP"](#)

SecurityFocus Bugtraq: [CERT-intexxia] libgtop_daemon Remote Fo

- ***Next in thread:*** Flavio Veloso: "Re: [CERT-intexxia] libgtop_daemon Remote Format String Vulnerability"
- ***Reply:*** Flavio Veloso: "Re: [CERT-intexxia] libgtop_daemon Remote Format String Vulnerability"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]