[**http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2448**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2448)

**Vulnerability Summary for CVE-2005-2448**

**Original release date:**08/03/2005

**Last revised:**08/21/2010

**Source:** US-CERT/NIST

**Overview**

Multiple "endianness errors" in libgadu in ekg before 1.6rc2 allow remote attackers to cause a denial of service (invalid behavior in applications) on big-endian systems.

**EKG Libgadu Multiple Memory Alignment Remote Denial of Service Vulnerabilities**

**http://ekg.chmurka.net/archive/**

I got the source from this site

**http://www.securityfocus.com/bid/14415/discuss**

EKG 'libgadu' is susceptible to multiple remote denial-of-service vulnerabilities.   
  
A malformed incoming message can trigger a bus error and lead to a crash.   
  
Note that these issues do not affect the application running on x86 architecture.

[**http://www.securityfocus.com/archive/1/406026**](http://www.securityfocus.com/archive/1/406026)

Multiple vulnerabilities have been found in libgadu, a library for   
handling Gadu-Gadu instant messaging protocol. It is a part of ekg, a   
Gadu-Gadu client, but is widely used in other clients. Also some of the   
user contributed scripts were found to behave in an insecure manner.  
  
Bugs fixed in ekg-1.6rc3:  
  
- integer overflow in libgadu (CAN-2005-1852) that could be triggered by  
an incomming message and lead to application crash and/or remote code  
execution (discovered by Marcin ¦lusarz),  
  
Bugs fixed in ekg-1.6rc2:  
  
- insecure file creation in user contributed Python script  
(CAN-2005-1916, discovered by Eric Romang of ZATAZ audit),  
  
- insecure file creation (CAN-2005-1850) and shell command injection  
(CAN-2005-1851) in other user contributed scripts (discovered by  
Marcin Owsiany and Wojtek Kaniewski),  
  
- several signedness errors in libgadu that could be triggered by an  
incomming network data or an application passing invalid user input to  
the library (discovered by Grzegorz Ja¶kiewicz),  
  
- memory alignment errors in libgadu that could be triggered by an  
incomming message and lead to bus errors on architectures like SPARC  
(discovered by Szymon Zygmunt and Micha³ Bartoszkiewicz),  
  
- endianness errors in libgadu that could cause invalid behaviour of  
applications on big-endian architectures (discovered by Marcin  
¦lusarz).  
  
Update is \*strongly\* recommended. The current version of ekg (including   
fixed libgadu) can be downloaded from:  
  
http://dev.null.pl/ekg/ekg-1.6rc3.tar.gz  
  
Note that due to frequent protocol modifications that require API and   
ABI changes, several Gadu-Gadu clients include libgadu in their source   
trees and use it as a static library. If you use Gadu-Gadu client based   
on libgadu other than ekg, please consult your vendor whether an update   
is necessary.  
  
Regards,  
Wojtek Kaniewski