

Re: Security Flaw in Popular Disk Encryption Technologies

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2008-02/msg00336.html>

- *From:* Jeremy Chadwick <koitsu@xxxxxxxxxxx>
 - *Date:* Sat, 23 Feb 2008 10:56:20 -0800
-

On Sat, Feb 23, 2008 at 07:40:53PM +0100, Pieter de Boer wrote:

Atom Smasher wrote:

article below. does anyone know how this affects eli/geli?
from the geli man page: "detach – Detach the given providers, which means remove the devfs entry and clear the keys from memory." does that mean that geli properly wipes keys from RAM when a laptop is turned off?

The attack you're referencing is carried out by cold rebooting a system. Simply put: pull power cord, insert power cord. The volumes are never detached, as the shutdown sequence is never run.

This attack has to be defended against in hardware; it exploits a 'feature' of modern day RAM chips, which can not be controlled by software. Anything that is in RAM when the attack is carried out, will be compromised. As encrypted volumes simply require keys to be in memory to be able to use the volumes, the encryption software is vulnerable to this attack. I see no reason why GELI/GBDE wouldn't be affected.

It's interesting that you classified this as a "feature" (in quotes), because there's nothing "modern" about said "feature". This issue has existed since the beginning of RAM chip engineering; I can even confirm this "feature" exists on old video game consoles such as the Nintendo and Super Nintendo (where there were strict guidelines put in place by Nintendo, requiring developers to initialise certain areas of memory and certain memory-mapped I/O registers during hard or soft resets).

A possible counter-measure would be to add wiping features to the RAM modules themselves. When power is lost, the memory could wipe itself. Still not perfect, but would certainly help.

Proper software should be `memset()` or `bzero()`'ing memory space it mallocs. I've gotten in the habit of doing this for years, purely as a safety net. If said software doesn't do this, it's very likely

Re: Security Flaw in Popular Disk Encryption Technologies

succeptable.

So the OP's question about ELI/GELI stands -- does it properly zero out memory it allocates before using it?

—
| Jeremy Chadwick jdc at parodius.com |
| Parodius Networking <http://www.parodius.com/> |
| UNIX Systems Administrator Mountain View, CA, USA |
| Making life hard for others since 1977. PGP: 4BD6C0CB |

freebsd-hackers@xxxxxxxxxxx mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-hackers>
To unsubscribe, send any mail to "freebsd-hackers-unsubscribe@xxxxxxxxxxx"