DSEC-2010-0001

Digit Security Security Advisory

Silicon Graphics Inc (SGI) - IRIX

Local Kernel Memory Disclosure/Denial of Service

Thursday 7th January, 2010

(generated on: Friday 15th April, 2011)

Local Kernel Memory Disclosure/Denial of Service - syssgi() XLV_ATTR_GET signedness vulnerability.

Tel: +44 (0)3300 881337
info@digit-security.com
digit-security.com

Contents

Vulnerability Summary

Vendor:	Silicon Graphics Inc (SGI)
Product:	IRIX
Affected Versions:	6.5.X
Vendor URL:	http://www.sgi.com/products/software/irix/

Author:	Neil 'mu-b' Kettle
CVE Reference:	CVE-2010-1692
BID #:	BID-45729
Severity:	Medium
Local/Remote:	Local
Vulnerability Class:	Denial of Service/Memory Disclosure/Privilege Escalation
Impact:	An attacker exploiting this vulnerability may access arbitrary kernel memory, or cause a Denial of Service attack via a page fault caused by an invalid pointer dereference resulting in a call to `panic()`.

1 Detailed Vulnerability Information

1.1 Introduction

A vulnerability has been discovered in the Silicon Graphics Inc (SGI) IRIX kernel, the vulnerability exists due to a signedness condition in the validation of a user-supplied array index value in the `syssgi` system call. Silicon Graphics Inc (SGI) documentation describes IRIX as:

"The IRIX® operating system is the leading technical high-performance 64-bit operating system based on industry-standard UNIX¨. For the past 20 years, SGI has been designing scalable platforms based on the IRIX operating system to connect technical and creative professionals to a world of innovation and discovery.

With IRIX, customers can take full advantage of MIPS® processor-based SGI® systems, ranging from visual workstations to advanced visualization systems and high-productivity supercomputers. IRIX 6.5 is SGI's fifth generation of IRIX and is one of the most important and mature UNIX operating system releases in the industry." [1]

1.2 Technical Background

A vulnerability exists due to a signedness condition in the validation of a user-supplied array index value in the `syssgi` system call. The vulnerable request value is `SGI_XLV_ATTR_GET` with a request attribute value of `XLV_ATTR_STATS`. The following code is the minimum required to reach the defective code within the IRIX kernel,

```
#include <sys/syssgi.h>
...
  xlv_attr_cursor_t tcursor;
  xlv_attr_req_t req;

  syssgi (SGI_XLV_ATTR_CURSOR, &tcursor);

  req.attr = XLV_ATTR_STATS;
  syssgi (SGI_XLV_ATTR_GET, &tcursor, &req);
```

The `syssgi` system call `SGI_XLV_ATTR_GET` request is a largely undocumented function, the Silicon Graphics Inc (SGI) man pages for the `syssgi` system call state the following with regard to the request value `SGI_XLV_*` family:

```
SGI_XLV_ATTR_CURSOR
SGI_XLV_ATTR_GET
SGI_XLV_ATTR_SET
SGI_XLV_NEXT_RQST
SGI_XLV_SET_TAB
  These are all interfaces that are used to implement various
  system library functions. They are all subject to change and
  should not be called directly by applications.
```

1.3 Vulnerability Details

The vulnerability is present in the `xlv_attr_get` function, part of which is given below,

```
kern/io/xlv/xlv_attr.c:
...
int
xlv_attr_get(xlv_attr_cursor_t *u_cursor,
             xlv_attr_req_t *u_req)
{
...
  } else if (k_cursor.subvol >= xlv_maxunits) {
    return(ENFILE);
  } else if (!xlv_tab->subvolume[k_cursor.subvol].vol_p) {
    return(ENOENT);
  }
  ASSERT(xlv_io_lock[k_cursor.subvol].statp);
  if (copyout(xlv_io_lock[k_cursor.subvol].statp,
    k_req.ar_statp, sizeof(xlv_stat_t))) {
    return(EFAULT);
  }
...
}
```

In the above code, the user controls the value of `k_cursor.subvol` which is declared as a `int`. As such, the `k_cursor.subvol >= xlv_maxunits` check is insufficient as `k_cursor.subvol` may be negative. The result of providing a large negative value for `k_cursor.subvol` will likely cause a kernel page fault upon dereferencing `xlv_tab->subvolume[...].vol_p`.

The vulnerability may also permit user access to arbitrary kernel memory since the user controls the value of `k_cursor.subvol` and thus the address of the `xlv_tab->subvolume[...].vol_p` and `xlv_io_lock[...].statp` dereferences leading to the source of the call to `copyout`.

1.4 Exploit Information

In order to trigger this vulnerability, a call to the `syssgi` system call is required with a signed (negative) `tcursor.subvol` value. The following code snippet will likely result in a kernel panic,

```
#include <sys/syssgi.h>
...
  xlv_attr_cursor_t tcursor;
  xlv_attr_req_t req;

  syssgi (SGI_XLV_ATTR_CURSOR, &tcursor);

  req.attr = XLV_ATTR_STATS;
  tcursor.subvol = 0xDEADBEEF; /* any value < 0 */
  syssgi (SGI_XLV_ATTR_GET, &tcursor, &req);
```

A proof of concept exploit can be obtained from digit-labs.org.

2 Vendor Response

Patches are available from the vendor to resolve these issues.

3 Recommendations

It is recommended that affected systems are updated to the latest patch level available from Silicon Graphics Inc (SGI), namely,

- patch7238 for IRIX 6.5.28
- patch7240 for IRIX 6.5.29
- patch7241 for IRIX 6.5.30

References

[1] Silicon Graphics Inc (SGI). SGI - Products: Software: IRIX. http://www.sgi.com/products/software/irix/, 2010.