Remediation Test of VPN Generator’s Application & Cryptography Architecture

EXECUTIVE SUMMARY

Engagement Details

<table>
<thead>
<tr>
<th>Client</th>
<th>VPN Generator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engagement Scope</td>
<td>Application &amp; Cryptography Architecture Review</td>
</tr>
<tr>
<td>Original Assessment Schedule</td>
<td>Jul 11, 2023 - Jul 28, 2023</td>
</tr>
<tr>
<td>Remediation Test Dates</td>
<td>Mar 6, 2024 - Mar 7, 2024</td>
</tr>
</tbody>
</table>

Remediation Test Update: Technical Findings Summary

The information below summarizes the observations of the Includesec team during the course of the remediation test intended to reproduce the findings as originally reported. The team attempted to bypass any added mitigations or protections put in place to hinder exploitation of the findings.

<table>
<thead>
<tr>
<th>Finding</th>
<th>Risk Rating</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>Low</td>
<td>Closed</td>
</tr>
<tr>
<td>L2</td>
<td>Low</td>
<td>Risk Accepted</td>
</tr>
<tr>
<td>L3</td>
<td>Low</td>
<td>Closed</td>
</tr>
<tr>
<td>L4</td>
<td>Low</td>
<td>Closed</td>
</tr>
</tbody>
</table>
LOW-RISK FINDINGS

L1: Secret Stored in Source Code Repository

*Status:* Closed

*Notes:*
This finding was retested and found to be remediated. The code base no longer contained any secrets stored in cleartext. The file identified in the original finding had been entirely removed from the folder, as can be seen from the output below, taken from the cloned repository.

```
$ pwd
[../]/ministry/conf
$ ls -hal
total 8.0K
  drwxr-xr-x 2 user user 4.0K Feb 6 19:53 ./
  drwxr-xr-x 9 user user 4.0K Feb 6 19:53 ../
  -rw-r--r-- 1 user user 0 Feb 6 19:53 keep-me
```

No other credentials were found elsewhere.

L2: Strict Host Key Checking Disabled

*Status:* Risk Accepted

*Notes:*
The VPN Generator team has accepted the risk for this finding with the following note:

*This situation is not considered critical as it pertains solely to our internal network infrastructure. All API interactions are securely managed through password authentication. Nevertheless, we acknowledge the necessity for enhancements in our security protocols. As we anticipate transitioning to a REST API in the near future, we plan to adopt an alternative system for identification. This system will either be based on x509 certificates or another simplified method, ensuring a more robust security framework.*

L3: Telegram Chat IDs Stored in Database

*Status:* Closed

*Notes:*
This finding was retested and found to be remediated. The `sessionID()` function now implemented an HMAC construction as per the recommendation in the original finding. The code snippet of the updated function can be seen below.

```go
func sessionID(secret []byte, chatID int64) []byte {
    var int64bytes [8 + len(sessionSalt)]byte
    binary.BigEndian.PutUint64(int64bytes[:8], uint64(chatID))
    copy(int64bytes[8:], sessionSalt)
    mac := hmac.New(sha256.New, secret)
    mac.Write(int64bytes[:])
    id := append([]byte(sessionPrefix), mac.Sum(nil)...)  
    return id
}
```
L4: Hosts Did Not Perform Automatic Updates

**Status:** Closed

**Notes:**

This finding was retested and found to be remediated. The `unattended-upgrades` package had now been installed and enabled as per the recommendation. The following screenshot demonstrates the configuration that was observed on all the relevant hosts.

```
Last login: Mon Feb 19 12:41:14 2024 from 10.20.128.2
ubuntu@preprod-2-vm-ct-100:~$ sudo -l
root@preprod-2-vm-ct-100:~# ps ax | grep unatt
    758  ?    0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
3962517 pts/1  S+   0:00 grep -F --color=auto unatt
root@preprod-2-vm-ct-100:~# dpkg -l | grep unatt
   ii: unattended-upgrades 2.8ubuntu
```

Note that the VPN Generator team stated that automating the reboot process was not desirable behavior for their circumstances; however, the assessment team believes the changes made are still sufficient to remediate this finding.