CVE-2016-1520: GrandStream Android VoIP App Update Redirection

Dr. Georg Lukas, rt-solutions.de GmbH, 2016-03-16

Affected app: *Grandstream Wave* version 1.0.1.26 (and probably earlier)

Classification:

- *CWE-300 Channel Accessible by Non-Endpoint*
- *CWE-319 Cleartext Transmission of Sensitive Information*
- CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H (score 6.4)

Summary

The Grandstream Wave app periodically queries the Grandstream server for app updates. If a new update is found, the app shows a notification to the user that either opens the app's Google Play page or auto-downloads the APK file and opens it for installation.

The update information is downloaded over an insecure connection from *media.ipvideotalk.com* and contains the version code and the update URL. An active attacker can redirect this request and trick the user into downloading a malicious update package. Users that have "Unknown Sources" enabled in the Android security preferences, or enable it upon request, can be tricked into installing a malicious application that disguises itself as a Wave update.

Details

The Grandstream Wave app downloads an update info XML on each app start. The address is hardcoded in the application properties as follows:

```
updateinfo_serverurl=http://media.ipvideotalk.com/upgrade/updateinfo.xml
```

This file was last updated in March 2015 and contains the following outdated information:

```
<?xml version="1.0" encoding="utf-8"?>
<info>
    <version>1.0.1.6</version>
    <versioncode>69</versioncode>
    <updateurl>market://details?id=com.softphone</updateurl>
    <description>检测到最新版本，请及时更新！</description>
</info>
```

The version available via Google Play at time of this writing is 1.0.1.26 (versioncode 89), therefore no update dialog will be shown by the application.

Internally, the XML is processed by the app as follows:

1. Check if the received *versioncode* is higher than the app's.
2. Prompt the user to install the update (figure 1).

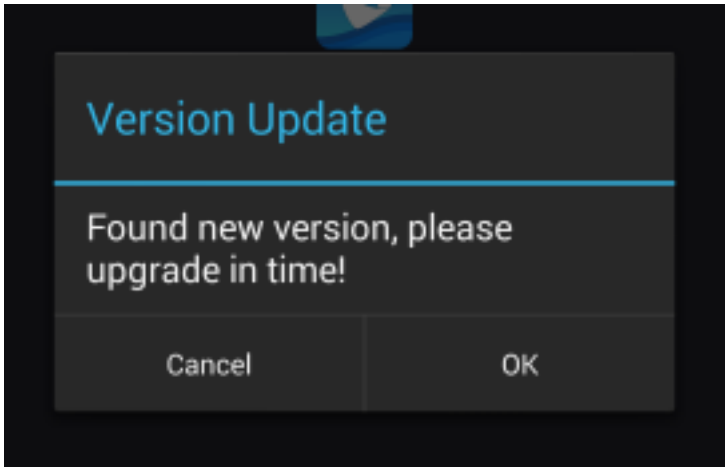

Figure 1: New Wave Version Dialog

3. If the `updateurl` contains `"market://details"`, open the Google Play page for the app's package (this is secure, the URL from the XML is not used).
4. Otherwise, download the file linked to by `updateurl` to `/sdcard/GSWave/upgrade/GSWave.apk` (figure 2) and open an installation dialog.

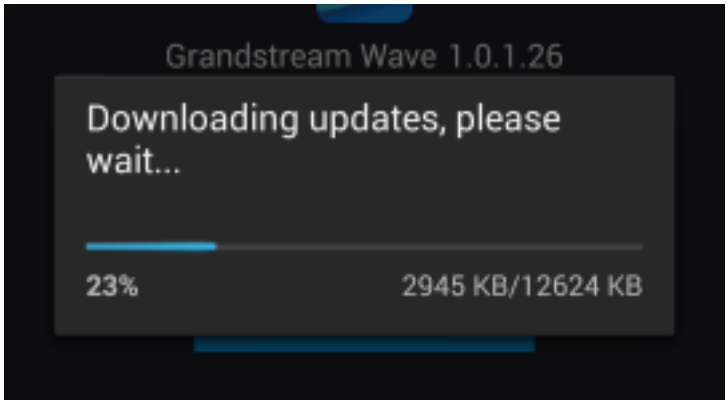

Figure 2: Download of New Version

5. If the user has "Unknown Sources" disabled, a warning dialog will be shown (figure 3) that forwards the user to the Android Security Preferences. If the user taps "Settings" and enables "Unknown Sources", the next update attempt will continue to step 6.

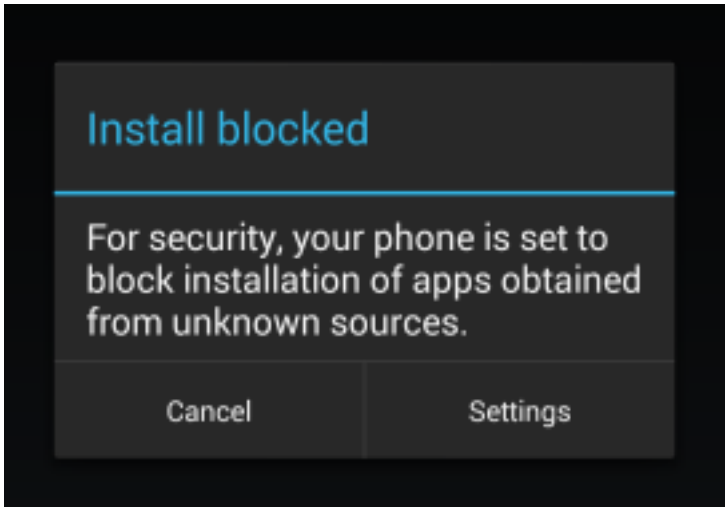

Figure 3: Android Security Settings

6. If "Unknown Sources" are allowed, Android will proceed with the app installation. For a normal user it is almost impossible to distinguish an official upgrade (figure 4) from a disguised malicious app (figure 5).

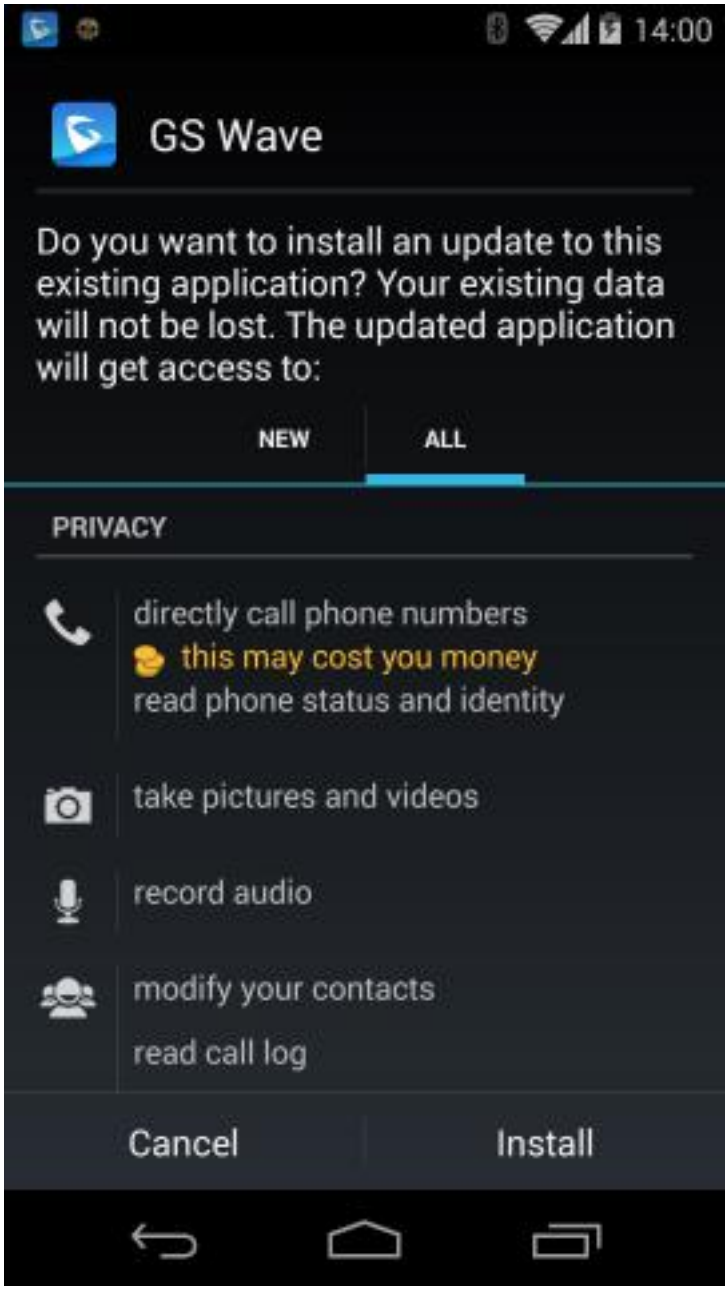

Figure 4: Upgrade of Official Wave App

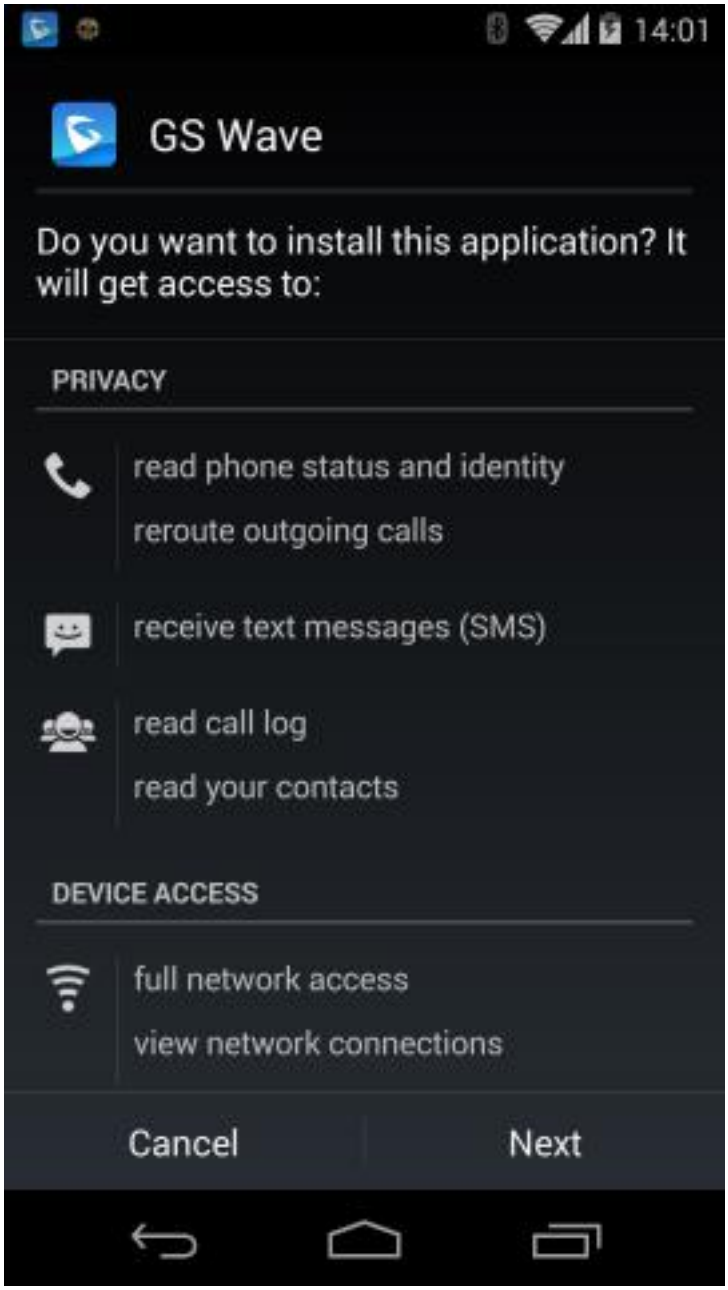

Figure 5: Installation of Malicious App

As from the user's perspective this is an update to a trustworthy app, which was initiated by the app itself, there is no reason to mistrust the installation and to question the permissions asked by the installer.

Impact

With a one-time Man-in-the-Middle attack, it is possible to trick the user into installing a malicious Android application with permissions to make phone calls, access the contact data, recording audio and video and much more. Such an application can perform extensive surveillance of the user afterwards.

Mitigation

It is not possible to disable update checks in the Wave application. Therefore, no technical mitigation mechanisms are possible. However, the following steps can be undertaken to reduce risk:

- Do not launch the Wave app on untrusted networks
- Use an automatic VPN connection to a trusted network
- Disable "Unknown Sources" in the Android security settings
- Inform the users not to install apps manually

Timeline

- 2015-11-25 Discovery of the issue
- 2015-11-25 Requested CVE number
- 2015-12-01 Notification of vendor
- 2016-01-20 CVE number assigned
- 2016-03-16 Public disclosure

Contact

Please contact *Dr. Georg Lukas* with any further questions regarding this vulnerability.