CVE-2016-1518: GrandStream Android VoIP Phone / App Provisioning Vulnerability

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

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

Affected device: Grandstream GXV3275 Android desk phone, version 1.0.3.55 (probably others as well)

Classification:

- CWE-300 Channel Accessible by Non-Endpoint
- CWE-319 Cleartext Transmission of Sensitive Information
- CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (score 8.1)

Summary

The Grandstream VoIP products deploy a remote provisioning mechanism that allows to automatically set configuration elements on phone/app startup. By default, an insecure connection to `fm.grandstream.com` is used to obtain the provisioning profile. An active attacker can redirect this request and change arbitrary values of the configuration. This allows to redirect phone calls through a malicious server, turn the phone into a bug, change passwords, and exfiltrate system logs (including the phone numbers dialed by the user). The changes are stored locally, so a single successful attack is sufficient to gain permanent control of the device.

Details

Grandstream devices are meant to be deployed in corporate environments, where central manageability is key. Therefore, they offer an auto-provisioning mechanism that allows central configuration of the VoIP and administrative settings, both in the physical products (Android-based desk phones like the GXV3275), and in the app deployed via Google Play (Grandstream Wave).

The auto-provisioning works by regularly downloading certain configuration files from a URL that is internally configured as the *Config Server Path*. The default *Config Server Path* is `http://fm.grandstream.com/gs/` which causes the phone/app to request provisioning data over an insecure channel from a server operated by Grandstream.

The desk phone downloads the configuration every 60 seconds, the app once on launch. Multiple configuration files are requested from the server, to allow specific and generic configuration:

- `cfg<MAC>` (desk phone only)
- `cfg<MAC>.xml` (desk phone and app)

- cfg.xml (desk phone and app)

cfg<MAC> is a plaintext file containing key-value pairs, cfg*.xml are XML files based on a similar key-value schema. <MAC> is the MAC address of the device, without byte delimiters.

Passive attackers can obtain the MAC address of the device running the VoIP application, as well as eventual provisioning elements returned by the server.

Active attackers can perform a Man-in-the-Middle attack (e.g. by means of ARP spoofing or DNS poisoning) to redirect the request to a maliciously crafted configuration file, re-provisioning the phone with new settings.

Impact

The provisioning file can change any aspect of the VoIP functionality. It contains key-value pairs for different options (Pxxx), e.g. the following to change the admin password (P2) and to redirect STUN traffic (P76):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<gs_provision version="1">
<config version="1">
<P2>haha-pwn3d</P2>
<P76>stun.mallory.evil</P76>
</config>
</gs_provision>
```

The GXV3275 phone has over 1600 different settings that can be configured this way, including:

- Changing of admin and user passwords
- Adding or replacing VoIP accounts / servers
- Turning the phone into a bug by setting a "silent" ringtone and enabling auto-answer
- Enabling syslog logging to an attacker-controlled server
- Changing the Config Server Path URL to a server controlled by the attacker, allowing to push new configuration after the initial Man-in-the-Middle attack

A full list of configuration options for different devices is available in the "Configuration Template" on the GrandStream server.

Mitigation

On the Wave app, the only way to close the issue is by disabling remote provisioning. This can be achieved by entering an empty URL:

1. Open "GSWave"
2. Switch to the "Settings" tab
3. Open "Advanced Settings" menu
4. Set "Config Server Path" to an empty string

On the GXV3275 desk phone, it is also possible to deploy secure provisioning by switching the provisioning mode to HTTPS and enabling certificate chain validation.

1. Open the administrative web interface
2. Switch to the "Maintenance" tab
3. Select the "Upgrade" menu
4. Set "Validate Certificate Chain" to "**Yes**"
5. Set "Upgrade Via" to "**HTTPS**"

After disabling / securing the auto-provisioning, **all configuration elements** should be checked for prior manipulation, e.g. by exporting and inspecting the phone configuration file.

Timeline

- 2015-11-24 Discovery of the issue
- 2015-11-24 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.