Remediating CVE-2011-3872 Via SSH

If you can trivially SSH to every node in your infrastructure, you can remediate the AltNames vulnerability by replacing your Puppet CA and causing every node to regenerate its SSL information. **This will permanently protect your site from master impersonation via the AltNames vulnerability.** This README contains step by step instructions for this fix.

These instructions should be carried out as root (or with high sudo privileges) on each affected system. This guide uses the command names introduced in Puppet 2.6; if you are using an older version of Puppet, the command names will differ as described at http://docs.puppetlabs.com/guides/tools.html. (Use puppetca instead of puppet cert, puppetd instead of puppet agent, and puppetmasterd instead of puppet master.)

To replace the CA and re-issue certificates, perform the following steps:

1. Stop all Puppet services
2. Disable `certdnsnames` on the puppet master and/or upgrade Puppet
3. Locate and delete the `ssldir` on the master and all agent nodes
4. Generate new certificates for the CA and the puppet master
5. Restart all Puppet services
6. Sign incoming certificate requests

Detailed instructions for each step follow.

1. Stop Puppet services

All agents should be stopped before you stop the puppet master. If you are running puppet agent as a daemon, you must stop the daemon; if you are running it from cron, you must move or disable the cron job for the duration of these steps.

When stopping the puppet master, be sure to both stop the puppet master processes and disable any supervisor process that manages the master. (For example, if you are running puppet master under Passenger, you should either stop Apache/Nginx, or restart the web server after moving the master's vhost config file to a disabled location.)

2. Disable `certdnsnames` and/or upgrade puppet master

To prevent Puppet from issuing dangerous certificates again, you must do one or both of the following:

- Disable the `certdnsnames` setting in the puppet master's puppet.conf
- Upgrade the puppet master to the most recent point release (2.6.12 or 2.7.6)

Note that `certdnsnames` may appear in the `[main], [master], [puppetmasterd],` or `[puppetca]` blocks of puppet.conf. To ensure that it is disabled, run the following command, which should return an empty line:

```
puppet master --configprint certdnsnames
```

If possible, you should also upgrade Puppet to the most recent point release. Puppet 2.6.12 and 2.7.6 have fixed the bug that produced this vulnerability, and will no longer issue dangerous certificates even if `certdnsnames` is turned on. They also feature an across-the-board improvement in the handling of DNS alt names; see the release notes for more details.

If you are using an older version of Puppet provided by your OS vendor, the vendor has likely provided an update that fixes this bug. Fixes to versions prior to the 2.6.x series disable `certdnsnames` functionality entirely, so if you absolutely require alternative DNS names in your puppet master certificate, you should delay upgrading until after step 4.

3. Locate and delete every `ssldir`

To delete the puppet master's `ssldir`, run:

```
rm -rf $(puppet master --configprint ssldir)
```

To delete the puppet agent's `ssldir`, run the following on every agent node:

```
rm -rf $(puppet agent --configprint ssldir)
```

4. Generate new CA and master certs

After the master's `ssldir` is gone, run the following command:

```
puppet cert --generate \
--ca_name "Puppet CA: Created on $(puppet master --configprint certname), <dat
e>" \
$(puppet master --configprint certname)
```

This will bootstrap a new CA and create a new master certificate. The `ca name` setting is arbitrary, but should be different from the default `ca_name` of "`Puppet CA: <master's certname>`".

If you are running 2.6.12/2.7.6 or later and need your master certificate to have alternative DNS names, modify the command as follows:

```
puppet cert --generate --dns_alt_names <comma-separated list of DNS names> \
--ca_name "Puppet CA: Created on $(puppet master --configprint certname), <dat
e>" \
$(puppet master --configprint certname)
```

If Puppet has **not** yet been updated, use the `--certdnsnames` option with a **colon-separated** list of names instead of the `--dns_alt_names` option. (Using `certdnsnames` is only safe in a one-time command like this.)

5. Restart all Puppet services

Restart the puppet master before re-enabling Puppet on any agent nodes.

6. Sign certificate requests

Your puppet agent nodes no longer have certificates, and each node will submit a certificate signing request on its first run. You will need to sign each request before your agent nodes can resume normal operation.

Use `puppet cert --list` to see a list of pending certificate requests, and `puppet cert --sign <certname> <certname>...` to sign any number of requests. You can sign all pending requests with `puppet cert --sign --all`.