CVE-2011-3872 Remediation Toolkit

This module will help you permanently remediate the CVE-2011-3872 AltNames vulnerability.

Usage Guides

Please see the detailed usage guides at:

- README-detailed.markdown (for remediating your site with Puppet)
- README-ssh-only.markdown (For remediating your site with SSH)

Summary

- If your puppet master's `certdnsnames` setting has **ever** been turned on, your site is at risk for attacks via the CVE-2011-3872 AltNames vulnerability.
- The AltNames vulnerability will persist even after Puppet has been updated to an unaffected version. It must be specifically remediated, either manually or with this helper module.

Am I Vulnerable?

If you have used `certdnsnames` on your puppet master, you are potentially vulnerable. All Puppet Enterprise users have used `certdnsnames` at some point.

To quickly test whether you are vulnerable, you can use the `scan certs` script included with this module. (Use the copy in `bin/` for Puppet Enterprise, and the copy in `bin/webrick` for open-source Puppet.)

```
 # bin/scan_certs

Status as of: 2011-10-23 19:42:26

                    Total Certificates Found:      7 *
                      Potentially Vulnerable:      7 (100.0%)
...
```

This script is not infallible, as it relies on the Puppet CA's certificate cache. If the cache has ever been deleted or modified, the script may return a false negative. You can also examine the local cert on any agent node by running:

```
openssl x509 -text -noout -in $(puppet agent --configprint hostcert)
```

...and looking for the X509v3 Subject Alternative Name field.

When in doubt, we recommend remediating the vulnerability.

How to Remediate CVE-2011-3872

You must fulfill two requirements to protect your site:

1. Disable puppet master's `certdnsnames` setting, and/or upgrade Puppet to an unaffected version.
2. Ensure that agents contact the master at a "clean" DNS name that has never been used as a subject alternative name by the site's CA.

There are multiple ways to meet the second requirement. You can:

- Pick a new DNS name and reconfigure all agents to use it

- Replace the CA and re-issue all certificates (so that ALL DNS names are "clean")
- Do both -- use a new DNS name for now, and clean your master's previous DNS name at your convenience

TO REMEDIATE YOUR SITE WITH PUPPET, see the README-detailed.markdown file included with this module.

TO REPLACE THE CA IMMEDIATELY WITH SSH, see the README-ssh-only.markdown file included with this module.

More Information

For more information about this vulnerability, including a FAQ, details about updated Puppet versions, and links to security hotfixes, go to: http://puppetlabs.com/security/cve/cve-2011-3872.