Acano solution

Security Alert Information

October 2016

76-1034-01-Aw

Acano is now part of Cisco.

acano

Contents

Introduction

This document details the Security alerts that Acano is aware of, and their workarounds (if any) and fixes. From 006 and onwards these alerts are graded according to the Common Vulnerability Scoring System (CVSS). The following Note and Disclaimer apply

Note: The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers should evaluate the impact of this vulnerability in their environments by accessing the CVSS guide (http://www.first.org/cvss/cvss-guide.html).

Disclaimer

The Forum of Incident Response and Security Teams (FIRST) states that the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of resonse". ACANO PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.

Known Security Issues that the Acano Solution is Not Affected By

CVE-2014-6271 “Shellshock”

Our Acano Solution is NOT affected by CVE-2014-6271 aka Shellshock as BASH is not included in the distribution used in our product.

CVE-2014-3566 “POODLE”

Our Acano Solution is NOT affected by CVE-2014-3566 aka POODLE: SSLv3 vulnerability as SSLv3 is turned off for web services in our product.

Security Alert 001 – NTP DDoS

Description

The Acano NTP service is based on the ntp.org reference implementation ntpd 4.2.6p5. By default, this version of NTP supports the `get monlist` command which can be exploited to amplify denial of service attacks [1], [2]. By sending `get monlist` commands with spoofed source addresses, an attacker can generate large volumes of response traffic targeted at a victim IP address. The Acano solution can therefore be used to amplify DDoS (Distributed Denial of Service) attacks; all network interfaces on the Acano solution can be queried for monlist data, therefore all interfaces are vulnerable.

Date

2014-02-11

CVE-ID

CVE-2013-5211

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano solutions running versions before 1.0.15.

Remediations and Fixes

Upgrade to version 1.0.15 or later.

Workarounds and Mitigations

Run systems behind a firewall with incoming UDP port 123 blocked. Test the firewall solution using nmap and the monlist module [3]. A vulnerable system will return results similar the following:

```
nmap -sU -pU:123 -Pn -n --script=ntp-monlist example.com
Starting Nmap 6.00 ( http://nmap.org ) at 2014-02-11 12:37 CET
Nmap scan report for example.com
Host is up (0.042s latency).
PORT    STATE SERVICE
123/udp open  ntp
| ntp-monlist:
|   Target is synchronised with 10.1.2.255
```

```
|   Alternative Target Interfaces:
|       169.254.1.0
|   Private Servers (1)
|       10.1.2.255
|   Private Clients (9)
|       10.1.2.117      169.254.2.0     169.254.2.4     169.254.2.8

|       10.1.3.169      169.254.2.2     169.254.2.6     169.254.2.10

|_      10.2.1.30

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Instead, running nmap on a system outside of the firewall should indicate that UDP port 123 is in the "open|filtered" or "closed" state.

References

[1] http://support.ntp.org/bin/view/Main/SecurityNotice#DRDoS_Amplification_Attack_using
[2] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5211
[3] http://nmap.org/nsedoc/scripts/ntp-monlist.html

Security Alert 002 – TLS heartbeat read overrun

Description

A serious vulnerability in the OpenSSL cryptographic software library: https://www.openssl.org/news/secadv_20140407.txt. By sending specially-crafted TLS heartbeat messages to a server which uses OpenSSL, an attacker can gather up to 64KB of potentially confidential data for each such message. Systems Affected

Acano is aware that the R1.0.18 (or earlier) and R1.1.3 (and earlier) code releases are impacted by the TLS heartbeat read overrun issue.

Date

2014-04-07

CVE-ID

CVE-2014-0160

CVSS Vector

(AV:N/AC:L/Au:N/C:P/I:N/A:N)

Affected Products and Versions

- Acano Solution versions < 1.0.19
- Acano Solution versions < 1.1.4

Remediation and Fixes

Upgrade to 1.0.19 or 1.1.4 or later. After upgrading, change all system passwords and recreate all certificates and keys.

Workarounds and Mitigations

There are no practical workarounds.

References

https://www.openssl.org/news/secadv_20140407.txt

http://heartbleed.com/

Security Alert 003 – Slowloris DoS vulnerability

Decription

Web services are vulnerable to a denial of service via partial HTTP requests known as the Slowloris 1.

Date

2014-08-08

CVE-ID

CVE-2007-6750

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P)

Affected Products and Versions

- Acano Solution versions < 1.1.8
- Acano Solution versions < 1.0.21

Remediation and Fixes

Upgrade to 1.0.21, 1.1.8 or later

Workarounds and Mitigations

No suggested workarounds, upgrade recommended.

References

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6750

Security Alert 004 – SSL/TLS MITM vulnerability

Description

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h do not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the CCS Injection vulnerability.

Date

2014-06-05

CVE-ID

CVE-2014-0224

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:P/A:P)

Affected Products and Versions

- Acano Solution versions < 1.1.8
- Acano Solution versions < 1.0.21

Remediation and Fixes

Upgrade to unaffected versions.

Workarounds and Mitigations

References

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224

http://www.openssl.org/news/secadv_20140605.txt

Security Alert 005 – DoS caused by failed authentication to the API or Web Admin Interface

Description

By making repeated failed authentication attempts to the API or Web Admin Interface, it is possible to degrade responsiveness to make the system difficult or impossible to use.

Date

2014-07-22

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

Acano Solution < 1.2.5

Remediation and Fixes

Upgrade to unaffected version.

Workarounds and Mitigations

Limit access to the Web Admin Interface and API by means of a firewall or a separate administration network.

Security Alert 006 – XMPP authentication succeeds with empty password if LDAP server allows 'unauthenticated authentication' method of simple bind

Description

If an XMPP client attempts to log in by sending a valid username and an empty password, and the LDAP server used for authentication allows the unauthenticated authentication method of simple bind, the login will succeed.

Date

2014-08-04

CVSS Vector

(AV:N/AC:M/Au:N/C:C/I:N/A:N/E:F/RL:OF/RC:ND)

Affected Products and Versions

- Acano Solution versions < 1.0.22
- Acano Solution versions < 1.1.10
- Acano Solution versions < 1.2.6

Remediation and Fixes

Upgrade to unaffected versions

Workarounds and mitigations

None

Security Alert 007 – OpenSSL vulnerabilities with Openssl 1.0.1i

Description

OpenSSL 1.0.1i addresses nine security vulnerabilities. Of these, five impacted the Acano solution.

Date

2014-08-29

CVE-ID

CVE-2014-3511 CVE-2014-3509 CVE-2014-3505 CVE-2014-3506 CVE-2014-3507

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.2.7

Remediation and Fixes

Upgrade to 1.2.7 or later

Workarounds and Mitigations

Some firewall products can mitigate this issue e.g.
https://techlib.barracuda.com/waf/configslowclientprevention

References

http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2014-3511&vector=(AV:N/AC:M/Au:N/C:P/I:N/A:N

http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2014-3509&vector=(AV:N/AC:M/Au:N/C:N/I:N/A:P

http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2014-3505&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:P

http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2014-3506&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:P

http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2014-3507&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:P

https://techlib.barracuda.com/waf/configslowclientprevention

Acknowledgement

OpenSSL Foundation

Security Alert 008 – Denial of service using partial HTTP requests

Description

By sending partial HTTP requests without closing the TCP connection to web services on the Acano solution, service can be denied to the Web Admin Interface and Web Bridge.

Date

2014-09-02

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.2.7

Remediationand Fixes

Upgrade to R1.2.7 or later

Workarounds and Mitigations

Some firewall products can mitigate this issue e.g.
https://techlib.barracuda.com/waf/configslowclientprevention

References

https://techlib.barracuda.com/waf/configslowclientprevention

Acknowledgement

University of Texas

Security Alert 009 – TLS denial of service

Description

A flaw in OpenSSL causes TLS servers to leak up to 64k of memory in response to a malicious TLS handshake. By repeating this operation, a malicious client could exhaust server memory causing a denial of service.

Date

2014-01-16

CVE-ID

CVE-2014-3513

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.2.11
- Acano Solution versions < 1.6.2.2

Remediation and Fixes

Upgrade to unaffected version

Workarounds and Mitigations

None

References

https://www.openssl.org/news/secadv_20141015.txt

Security Alert 010 – WebRTC guest user DoS

Description

By creating very large numbers of slave devices, a WebRTC guest could prevent users from joining coSpaces.

Date

2014-11-13

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:U/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.2.13
- Acano Solution versions < 1.6.5

Remediation and Fixes

Upgrade to unaffected version

Workarounds and Mitigations

None

Security Alert 011 – coSpace activated in error by guest-initiated chat

Description

A coSpace can be activated by a guest if a Lync client user is a guest in the coSpace.

Date

2014-11-13

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:N/A:N/E:H/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.2.13
- Acano Solution versions < 1.6.5

Remediation and Fixes

Upgrade to unaffected version

Workarounds and mitigations

None

Security Alert 012 – Deployment guide suggested insecure XMPP server settings

Description

The Deployment Guide incorrectly suggest that port 5269 be used in the XMPP setting set through the web admin interface. The correct port is 5223. Using 5269 results in XMPP component connection traffic between the callbridge and the XMPP server being transmitted in plain text.

Date

2014-11-13

CVSS Vector

(AV:A/AC:M/Au:N/C:P/I:P/A:N)

Affected Products and Versions

- Acano Documentation versions < 76-1006-06-E

Remediation and Fixes

On the Web Admin Interface page **Configuration > General**, change the port in XMPP Server Settings to 5223.

Workarounds and Mitigations

On the Web Admin Interface page **Configuration > General**, change the port in XMPP Server Settings to 5223.

Security Alert 013 – Invalid XML in client XMPP stream causes dropped client connections

Description

XMPP server fails to correctly sanitize XML received from clients before forwarding to XMPP components. This can cause all active connections to be dropped.

Date

2014-12-17

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:S/C:N/I:N/A:P/E:POC/RL:U/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.2.13
- Acano Solution versions < 1.6.9

Remediation and Fixes

Upgrade to unaffected version.

Workarounds and Mitigations

None.

Security Alert 014 – Multiple NTP vulnerabilities

Description

The Acano solution uses ntp-keygen to generate client keys to support autokey. ntp-keygen uses a non-cryptographic random number generator to generate symmetric keys making them easy to guess.

Multiple buffer overflow flaws were discovered in ntpds crypto_recv(), ctl_putdata(), and configure() functions. Acano X series servers are vulnerable to overflows in crypto_recv(). An attacker could, using a specially-crafted NTP packet cause a denial of service (disrupt accurate time keeping) or execute arbitrary code. Successful arbitrary code execution is made more difficult by address space layout randomization; successful execution of code would have limited impact due to sandboxing of the ntp process. ctl_putdata() and configure() flaws do not impact the Acano solution.

Date

2014-12-18

CVE-ID

CVE-2014-9294 and CVE-2014-9295

CVSS Vector

(V:N/AC:L/Au:N/C:P/I:P/A:P)

Affected Products and Versions

- Acano Solution versions 1.6.x where x is less than and equal to 9
- Acano solution version 1.1 and 1.2 are not affected

Remediation and Fixes

Upgrade to an unaffected version when available, which will be the next maintenance release of 1.6

Workarounds and Mitigations

Create local firewall rules using MMP commands (see the MMP Command Reference).

For Acano X series servers use

```
firewall admin default allow
firewall admin deny ntp/udp
```

```
firewall admin enable
```

For Acano VMs use:

```
firewall a default allow
firewall a deny ntp/udp
firewall a enable
firewall b default allow
firewall b deny ntp/udp
firewall b enable
firewall c default allow
firewall c deny ntp/udp
firewall c enable
firewall d default allow
firewall d deny ntp/udp
firewall d enable
```

Note: That this will prevent normal operation of NTP; however you can still set the system time. After upgrade to an unaffected version, remove the firewall rules.

References

1. http://www.kb.cert.org/vuls/id/852879
2. http://support.ntp.org/bin/view/Main/SecurityNotice

Security Alert 015 – Role enforcement in Web Admin Interface login

Description

Only MMP account users with admin and appadmin roles should be able to login to the Web Admin Interface. MMP account users with other roles (crypto, audit and api) should not be able to access the Web Admin Interface.

Date

2014-12-20

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:S/C:P/I:P/A:P)

Affected Products and Versions

- Acano Solution versions 1.6.x where x is less than and equal to 9
- Acano Solution versions < 1.2.x where x is less than and equal to 13

Remediation and Fixes

Upgrade to unaffected version of your release when available. Release 1.6.10 is now available.

Workarounds and Mitigations

Run the user expire MMP command on users with roles other than admin and appadmin to prevent those users logging in. See the MMP Command Reference.

Security Alert 016 – DTLS Denial of Service

Description

Prior to 1.0.1k OpenSSL is vulnerable to a denial of service, caused by a NULL pointer dereference when handling malicious messages. By sending a specially-crafted DTLS message, a remote attacker could exploit this vulnerability to cause a segmentation fault.

In addition, a memory leak can occur in the dtls1_buffer_record function under certain conditions. In particular, this could occur if an attacker sent repeated DTLS records with the same sequence number but for the next epoch. The memory leak could be exploited by an attacker in a Denial of Service attack through memory exhaustion.

Date

2015-01-08

CVE-ID

CVE-2014-3571 CVE-2015-0206

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.6.10
- Acano Solution versions < 1.2.14

Remediation and Fixes

Upgrade to 1.6.10 (now available) or to 1.2.14

Workarounds and Mitigations

None

References

1. https://www.openssl.org/news/secadv_20150108.txt

Security Alert 017 – Open URL redirection vulnerability

Description

If acano.example.com is the URL of an Acano server's Web Admin Interface, then the link

`https://acano.example.com/authentication?url=http://www.google.com`

will redirect the user to www.google.com after clicking through authentication (successful or not). This could be exploited to gather credentials from an unsuspecting user. See the reference below.

Date

2015-01-16

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.6.11
- Acano Solution versions < 1.2.14

Remediation and Fixes

Upgrade to an unaffected version.

Workarounds and Mitigations

None

References

1. https://www.owasp.org/index.php/Open_redirect

Security Alert 018 – Web Admin XSS Vulnerability from authentication page

Description

If acano.example.com is the URL of an Acano servers Web Admin Interface, then the link

```
https://acano.example.com/authentication?url=%2f%27;alert(%27xss%27);var%20x%3d%27
```

will result in execution of javascript to create a popup with the text xss after clicking through authentication (successful or not).

Date

2015-01-16

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano solution versions <1.6.11
- Acano solution versions <1.2.14

Remediation and Fixes

Upgrade to an unaffected version

Workarounds and Mitigations

None

References

1. https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

Security Alert 019 – Role enforcement in HTTP API authentication

Description

Only admin, appadmin and api roles should be able to perform task with the HTTP API. In vulnerable versions, all user roles could perform operations using the HTTP API.

Date

2015-01-16

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:S/C:P/I:P/A:P)

Affected Products and Versions

- Acano Solution versions < 1.6.11

Remediation and Fixes

Update to an unaffected version.

- Acano Solution versions > 1.6.10

Workarounds and Mitigations

Use user expire on roles other than admin and appadmin will prevent those user logging in..

Security Alert 020 – Ghost security vulnerability

Description

Buffer overflow in __nss_hostname_digits_dots in versions of eglibc < 2.18 can cause memory corruption, and allow arbitrary code execution. This call is used primarily by gethostbyname() and gethostbyname2() which allow a remote attacker to exploit this vulnerability.

Date

2015-01-28

CVE-ID

CVE-2015-0235

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:P/A:P)

Affected Products and Versions

- Acano Solution versions < 1.2.15
- Acano Solution versions < 1.6.12

Remediation and Fixes

Update to an unaffected version. Both 1.6.12 and 1.2.15 are currently available.

Workarounds and Mitigations

None.

Security Alert 021 – Database enabled erroneously

Description

An Acano server connected to a database cluster (not a member of the cluster) will, after a reboot, have the database enabled on port 5432. Remote access to the database using postgres default null credentials is then possible.

Date

2015-03-11

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:P/A:N/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano solution versions <1.6.18
- Acano solution versions 1.7(Beta1)

Remediation and Fixes

Upgrade to an unaffected version

- Acano solution versions >1.6.17
- Acano solution versions >1.7(Beta1)

Workarounds and Mitigations

Enable the server firewall to block connections e.g.

```
acano> firewall a default allow
acano> firewall a deny 5432
acano> firewall a enable
```

To test that the port is blocked correctly, using nmap

```
nmap -p 5432 acano.example.com
```

Security Alert 022 – OpenSSL vulnerability CVE-2015-0286

Description

OpenSSL before 1.0.1m is vulnerable to a denial of service attack where an attacker presents a certificate to the client or server which, while being validated, causes a crash.

This can happen in the following circumstances:

- the client connects to a malicious host (client crash)
- the server connects to a malicious server (server crash)
- a malicious client presents a crafted client certificate to the CAC enabled server (server crash)
- TLS connection to the webbridge using SNI for the API service with a malicious client authentication certificate (webbridge crash)

Date

2015-03-19

CVE-ID

CVE-2015-0286

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:POC/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.2.19
- Acano Solution versions < 1.5.2
- Acano Solution versions < 1.6.19
- Acano Clients versions < 1.3.55

Remediation and Fixes

Upgrade to an unaffected version

- Acano solution versions >1.6.18
- Acano solution versions >1.7(Beta2)
- Acano Clients > 1.6.29

Workarounds and Mitigations

Acano recommends the use of DNSSEC to protect infrastructure servers from man-in-the-middle attacks. Protection for the webbridge requires upgrading software to an unaffected version.

Security Alert 023 – Information leak via misconfigured webbridge

Description

Webbridge mistakenly listens on port 54321. The webbridge application, without the protection of the HTTP security proxy, allows files on the root filesystem to be read.

Date

2015-06-04

CVSS Vector

(AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions 1.7.0, 1.7.1 and 1.7.2

Remediation and Fixes

Implement workaround until next maintenance release following 1.7.2

Workarounds and Mitigations

Enable the server firewall to block connections e.g.

```
acano> firewall a default allow
acano> firewall a deny 54321
acano> firewall a enable
acano> firewall b default allow
acano> firewall b deny 54321
acano> firewall b enable
acano> firewall c default allow
acano> firewall c deny 54321
acano> firewall c enable
acano> firewall d default allow
acano> firewall d deny 54321
acano> firewall d enable
```

To test that the port is blocked correctly, using nmap

```
nmap -p 54321 acano.example.com
```

Security Alert 024 – Multiple OpenSSL vulnerabilities prior to 1.0.1n

Description

OpenSSL 1.0.1n addresses seven security vulnerabilities. Of these, the five listed below impacted the Acano solution.

Date

2015-06-11

CVE-ID

CVE-2015-4000, CVE-2015-1788, CVE-2015-1789, CVE-2015-1791, CVE-2014-8176

CVSS Vector

(AV:N/AC:H/Au:N/C:P/I:N/A:P/E:POC/RL:OF/RC:C/CDP:ND/TD:ND/CR:ND/IR:ND/AR:ND)

Affected Products and Versions

- Acano Solution versions < 1.6.22
- Acano Solution versions <1.7.3
- Acano Clients versions < 1.6.33

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 025 – SDP Denial of Service

Description

A vulnerability in the Session Descriptor Protocol (SDP) parser of the callbridge could allow an unauthenticated, remote attacker to cause the parsing process to crash.

Date

2015-06-29

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.6.23
- Acano Solution versions <1.7.5

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 026 – XMPP Authentication Denial of Service

Description

During authentication of Acano clients, the XMPP server can be made to crash with a currently undisclosed attack vector. Note that the attacker does not require valid authentication credentials for success.

Date

2015-06-29

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions < 1.6.23
- Acano Solution versions <1.7.5

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 027 – OpenSSL Leaf Node CA validation

Description

OpenSSL 1.0.1p addresses a single high level security vulnerability which affects the Acano solution, where an attacker can cause certificates to be incorrectly validated exposing the user to a Man-In-The-Middle attack.

Date

2015-07-09

CVE-ID

CVE-2015-1793

CVSS Vector

(AV:A/AC:L/Au:N/C:C/I:C/A:C/E:ND/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions 1.6.22 and 1.6.23
- Acano Solution versions 1.7.3,1.7.4 and 1.7.5
- Acano Clients versions 1.7.9 and 1.7.10

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

References

1. https://openssl.org/news/secadv_20150709.txt

Acknowledgements

OpenSSL foundation

Security Alert 028 – Unencrypted media used between Call Bridges

Description

Media between clustered Call Bridges can be sent unencrypted. This potentially allows eavesdropping of meetings if an attacker can access the network between the Call Bridges.

Date

2015-07-10

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:U/RC:C)

Affected Products and Versions

- Acano Solution versions <1.7.6

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 029 – DHCPv6 Options Buffer Overflow

Description

Acano infrastructure products use dhcpcd to provide support for DHCPv6. A buffer overflow in DHCPv6 options parsing allows remote DHCP servers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted message.

Date

2015-08-03

CVE-ID

CVE-2014-7913

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:P/A:P)

Affected Products and Versions

- Acano Solution versions <1.6.26
- Acano Solution versions <1.7.8

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

Disable SLAAC support for the network interfaces. IPv6 support in general is disabled by default and so no action is required unless IPv6 is in use.

Security Alert 030 – SSH connection persists after max authentication attempts exceeded

Description

OpenSSH does not properly restrict the processing of keyboard-interactive devices within a single connection. As a consequence, an attacker can reuse a single SSH connection to make multiple attempts at brute force guessing of passwords. Note that the interval between failed attempts is still enforced (four seconds) so the only advantage gained here is removing the overhead of creating a new SSH connection.

Date

2015-07-23

CVE-ID

CVE-2015-5600

CVSS Vector

(AV:N/AC:L/Au:N/C:P/I:N/A:N)

Affected Products and Versions

- Acano Solution versions <1.6.25
- Acano Solution versions <1.7.7

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

Our recommended practices will mitigate this vulnerability:

- enable enforcement of passwords complexity
- restrict user logins to known hosts
- enable duty hours
- enable account lockout
- use strict Common Access Card mode (works for normal SSH public keys)

Security Alert 031 – Webbridge Denial of Service

Description

Debug functionality could be exploited by remote, unauthenticated attackers to restart the webbridge.

Date

2015-08-18

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:C)

Affected Products and Versions

- Acano Solution versions <1.6.26
- Acano Solution versions <1.7.8

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 032 – A user can join as host using the guest callID if already logged in as a user

Description

If a user is logged in with the Acano client and follows an invitation link to a webbridge and selects to use the Acano client, the user will enter the cospace as host.

Date

2015-09-14

CVE-ID

Pending

CVSS Vector

(AV:N/AC:H/Au:M/C:P/I:N/A:N/E:POC/RL:OF/RC:ND)

Affected Products and Versions

- Acano Solution versions <1.6.29
- Acano Solution versions <1.7.11

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 033 – Media process restarts when OCS 2007 R2 clients share content in coSpace

Description

When OCS 2007 R2 clients share content, an assert is triggered which causes the media process to restart.

Date

2015-09-14

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions <1.6.29
- Acano Solution versions <1.7.11

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 034 – XMPP pubsub information disclosure

Description

Pubsub nodes subscription is not properly controlled by a whitelist. This allows authenticated users to see data belonging to other users.

Date

2015-09-14

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:S/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions <1.6.30
- Acano Solution versions <1.7.12
- Acano Solution versions <1.8.1

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 035 – Persistent cross-site scripting

Description

User names presented in the participant list when using the WebRTC client are not properly sanitized. A user entering as a guest can choose a name which will be rendered as HTML.

Date

2015-09-14

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:S/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions <1.6.30
- Acano Solution versions <1.7.12
- Acano Solution versions <1.8.1

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 036 – Windows Client HTML anchor tags rendering

Description

The Acano Windows client renders a subset of HTML, which includes anchor tags. When setting the href attribute of an anchor tag to a file:// URI pointing to an executable binary this binary will be executed without further confirmation when clicked by the user.

Date

2015-09-14

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Affected Products and Versions

- Acano Clients versions <1.8.8

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 037 – Memory corruption caused by custom URI handler

Description

On the Microsoft Windows platform, users joining a conference via the webbridge can opt to use the native client. For this client a custom acano: URI handler will be installed. Insufficient bounds checking on this string can lead to memory corruption.

Date

2015-09-14

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:S/C:P/I:P/A:C/E:POC/RL:OF/RC:C)

Affected Products and Versions

- Acano Clients versions <1.8.8

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 038 – XMPP Man In The Middle

Description

A man in the middle can through unspecified means cause XMPP nodes (Acano clients and infrastructure) to fail to negotiate a TLS connection and proceed to send data as plaintext.

Date

2015-10-08

CVE-ID

Pending

CVSS Vector

(AV:N/AC:H/Au:N/C:C/I:C/A:N)

Affected Products and Versions

- Acano Clients versions <1.7.14
- Acano Solution versions <1.6.31
- Acano Solution versions <1.7.13
- Acano Solution versions <1.8.2

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None

Security Alert 039 – Multiple NTPd vulnerabilities

Description

ntp 4.2.8p4 addresses thirteen security vulnerabilities, of which six affect the Acano Server. These vulnerabilities can cause denial of service of the ntp service as well as allowing an attacker to control the reference time on the Acano Server.

Date

2015-10-21

CVE-ID

CVE-2015-7691 CVE-2015-7692 CVE-2015-7702 CVE-2015-7704 CVE-2015-7705 CVE-2015-7701 CVE-2015-7854 CVE-2015-7855 CVE-2015-7871

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:P/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions <1.6.32
- Acano Solution versions <1.7.14
- Acano Solution versions <1.8.3

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

To mitigate some of the vulnerabilities a user can disable incoming NTP traffic until they are ready to upgrade to an unaffected version.

Create local firewall rules. For hardware Acano solution servers

```
firewall admin default allow
firewall admin deny ntp/udp
firewall admin enable
```

For Acano solution VMs

```
firewall a default allow
```

```
firewall a deny ntp/udp
firewall a enable
firewall b default allow
firewall b deny ntp/udp
firewall b enable
firewall c default allow
firewall c deny ntp/udp
firewall c enable
firewall d default allow
firewall d deny ntp/udp
firewall d enable
```

Note that this will prevent normal operation of NTP.

References

1. http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities
2. http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-ntp
3. http://blog.talosintel.com/2015/10/ntpd-vulnerabilities.html
4. http://www.cs.bu.edu/~goldbe/NTPattack.html

Security Alert 040 – Crash processing large numbers of SRV records

Description

Services can crash if a DNS SRV resolution results in a large number of records. Since DNS resolutions can be triggered by interactions with remote parties, this constitutes a denial of service vector.

Date

2015-11-24

CVSS Vector

(AV:N/AC:M/Au:N/C:N/I:N/A:C)

Affected Products and Versions

- Acano Solution versions <1.7.16
- Acano Solution versions <1.8.5

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

Security Alert 041 – Multiple OpenSSL vulnerabilities prior to 1.0.1q

Description

OpenSSL 1.0.1q addresses four security vulnerabilities. Of these, CVE-2015-3194 is known to make Acano products vulnerable to a denial of service attack.

Date

2015-12-03

CVE-ID

CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:C)

Affected Products and Versions

- Acano Solution versions <1.7.16.1
- Acano Solution versions <1.8.5.1

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

References

3. https://www.openssl.org/news/secadv/20151203.txt

Acknowledgements

OpenSSL Foundation

Security Alert 042 – Multiple Webbridge XSS vulnerabilities

Description

Improper use of JQuerys html 1 method leads to untrusted input being rendered as HTML.

Date

2016-02-03

CVE-ID

Pending

CVSS Vector

AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

Affected Products and Versions

- Acano Solution versions <1.7.19
- Acano Solution versions <1.8.9

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

References

1. http://api.jquery.com/html/

Acknowledgements

Vodafone

Security Alert 043 – Webbridge Denial of Service: large HTTP headers

Description

Parsing large HTTP headers could lead to worker threads blocking and degradation of service.

Date

2016-02-03

CVE-ID

Pending

CVSS Vector

AV:N/AC:L/Au:N/C:N/I:N/A:C

Affected Products and Versions

- Acano Solution versions <1.7.18
- Acano Solution versions <1.8.8

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

If the webbridge is deployed behind an HTTP proxy, limit the size of HTTP headers accepted by the proxy to less than 6KB.

Acknowledgements

British Telecom

Security Alert 044 – DHCPCD vulnerabilities

Description

Acano Server uses dhcpcd for IPv6 SLAAC and DHCPv6 which has memory corruption issues handling malformed DHCP responses.

Date

2016-04-26

CVE-ID

CVE-2016-1503

CVSS Vector

(AV:N/AC:L/Au:N/C:C/I:C/A:C)

Affected Products and Versions

- Acano Solution versions <1.7.22
- Acano Solution versions <1.8.13

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

Disable IPv6 auto-configuration.

Security Alert 045 – SRTP denial of service

Description

A crafted RTP header containing a falsified CSRC count/header extension flag may can cause a denial of service.

Date

2016-04-22

CVE-ID

CVE-2015-6360

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions <1.7.21
- Acano Solution versions <1.8.12

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-libsrtp

Security Alert 046 – Conference locking race condition

Description

In a clustered deployment, it is possible for a guest user to bypass the lobby of a locked space. In particular, if the guest login is handled by a call bridge which has never hosted the space, then the guest may bypass the lobby.

Date

2016-02-22

CVE-ID

Pending

CVSS Vector

(AV:N/AC:M/Au:N/C:P/I:N/A:N/E:H/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions <1.8.13

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

Security Alert 047 – SIP denial of service

Description

A malicious SIP client can cause callbridge crashes by selecting AAC-LC audio codec.

Date

2016-04-12

CVE-ID

Pending

CVSS Vector

(AV:N/AC:L/Au:N/C:N/I:N/A:C)

Affected Products and Versions

- Acano Solution versions <1.7.22
- Acano Solution versions <1.8.12

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

Security Alert 048 – Multiple NTP vulnerabilities

Description

The Acano server uses ntpd to provide Network Time Protocol support. A recent release addresses multiple vulnerabilities.

Date

2016-04-28

CVE-ID

CVE-2016-1551 CVE-2016-1549 CVE-2016-2516 CVE-2016-2517 CVE-2016-2518 CVE-2016-2519 CVE-2016-1547 CVE-2016-1548 CVE-2015-7704 CVE-2015-8138 CVE-2015-1550

CVSS vector

(AV:N/AC:L/Au:N/C:N/I:P/A:P)

Affected Products and Versions

- Acano Solution versions <1.7.22
- Acano Solution versions <1.8.13

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

Security Alert 049 – Open SSL Padding Oracle in AES-NI CBC MAC check

Description

When using OpenSSL versions prior to 1.0.1t a man-in-the-middle (MITM) attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI. This impacts the Acano hardware solution which uses Intels AES-NI acceleration.

Date

2016-05-03

CVE-ID

CVE-2016-2107

CVSS vector

(AV:N/AC:H/Au:N/C:P/I:P/A:N)

Affected Products and Versions

- Acano Solution versions <1.7.22
- Acano Solution versions <1.8.13
- Acano PC client versions < 1.8.30
- Acano iOS client versions < 1.8.2

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

Security Alert 050 – NTP denial of service vulnerability

Description

A spoofed CRYPTO_NAK response could cause the NTP service to crash.

Date

2016-06-02

CVE-ID

CVE-2016-4957

CVSS vector

(AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Affected Products and Versions

- Acano Solution versions <1.7.23
- Acano Solution versions <1.8.14
- Acano Solution versions <1.9.1

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

None.

Security Alert 055 – XMPP authentication bypass

Description

A vulnerability in the Extensible Messaging and Presence Protocol (XMPP) service of the Acano Server could allow an unauthenticated, remote attacker to masquerade as a legitimate user. This vulnerability is due to the XMPP service incorrectly processing a deprecated authentication scheme. A successful exploit could allow an attacker to access the system as another user.

For more details see https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-msc

Date

2016-10-12

CVE-ID

CVE-2016-6445

CVSS vector

(AV:N/AC:L/Au:N/C:P/I:P/A:N/E:POC/RL:U/RC:C)

Affected Products and Versions

- Cisco Meeting Server versions <2.0.6
- Acano Solution versions <1.9.6
- Acano Solution versions <1.8.18

Remediation and Fixes

Upgrade to unaffected release

Workarounds and Mitigations

Disable XMPP service.

Acknowledgement

Administrative Office of the US Courts