

Vendor: Alcatel  
 Affected Products: Versions before 9.0.8.4 of the CCAgent option of  
 OmniTouch Contact Center Standard Edition  
 Vulnerability: unauthenticated administrative access to CTI CCA Server  
 Risk: High  
 CVE-Number: CVE-2010-3279 (unauthenticated maintenance access)  
 and CVE-2010-3280 (user credentials disclosure)

## Vendor communication:

2010/02/16 initial information to Alcatel-Lucent from n.runs AG  
 2010/02/16 initial response from Alcatel-Lucent to investigate  
 responsibility within Alcatel-Lucent group  
 2010/02/18 request from Alcatel-Lucent about former vendor communication  
 2010/02/18 response given to n.runs at the end of 2009 from a customer  
 that requested n.runs to take over the handling of the  
 vulnerability and to publish it.  
 2010/02/24 confirmation from Alcatel-Lucent that vulnerability exists  
 2010/03/15 n.runs confirms CVSS rating  
 2010/08/10 Alcatel-Lucent confirms that vulnerability is fixed  
 (fix date: 2010/06/08)  
 2010/08/23 Alcatel-Lucent proposes September 15th as the publication date  
 and request CVE number  
 2010/09/13 Business Partners of Alcatel-Lucent are informed about the  
 vulnerability  
 2010/09/15 CVE numbers received  
 2010/09/20 n.runs AG releases this advisory

## Overview:

Alcatel offers a CTI Solution for Call Centers. Call-Center Agents can log on to the central CCA-Server with a helper client and can redirect calls from their call center extension to a normal phone even while they are out of office.

## Description:

Besides the tracking and managing of all connected agents with their computers and phones, the server also has remote management and debugging facilities for administrators.

For the administration of the server the same tcp/ip ports are used for the registration of the out of office call center agents.

In addition there is no real authentication taking place. A tool called "Tsa\_Maintenance.exe" that ships with the product, can be used to view the debugging functions and status of the call center without any authentication. This way every call center agent can monitor the entire call-center, co-workers, can trace lines, deregister lines, etc...

Further investigation showed that there is authentication available but it is implemented in the wrong way. In a normal setup, the client is sending the credentials to the server for verification.

The ALCATEL WAY of user authentication is that the client verifies if authentication was successful. The call center agent server is sending the administrative password to the client in order to enable the client to decide to go on to the administrative functions or not. Therefore it is trivial to patch the client software to pass the authentication. Furthermore with every "authentication" attempt to the server the attacker gains knowledge of the administrative password.

The password for the "SuperUser" is sent from the TSA server to the client in cleartext in the following way:

Name=SuperUser Password=072 175 173 176 173 177 181

Well, it is exactly as it appears above. It is the "SuperUser"'s account name and password, which is somehow obfuscated. The first number (72) is the offset of the rest of numbers to the ascii decimal representation of the password character.

175 - 72 = 103 == g  
173 - 72 = 101 == e  
...

The above password in cleartext is called "geheim" (german for: secret)

This password authentication scheme is an epic failure in terms of design.

#### Impact:

-----  
The problems described allow an attacker to basically do whatever he or she wants to with the call-center. From monitoring to completely reconfiguring it and disrupting service. Everything is possible.

#### Solution

-----

##### Workaround

Disable the maintenance access:

- On the TSA server: disable the TSA maintenance access in the server configuration file.

##### Mitigation

Implement segregation of roles:

- Agent workstations should not propose the manager's client application (TSA\_manager.exe). Remove it if found.
  - Manager workstations should only propose the manager's client application and not the agent client application.
  - Use a separate IP subnet to host the manager workstations.
  - Provide physical protection to manager workstations by implementing physical access control to the room where the Contact Center managers have their workstations.
- Protect credential exchanged over the LAN:
- Configure IPsec on the TSA server to require mandatory IPsec access from an explicit list of management workstations.
  - Configure the windows firewall to allow cleartext accesses from an explicit list of agent workstations and drop all packets from any other workstations.
- Fixed Software Versions/Patches and how to obtain them  
CCAgent version 7.1 and before are no longer supported. Users must upgrade to the most recent CCAgent version.

---

#### Credits:

Bug found by Axel Rengstorf of Bluebox Security and Florian Walther of n.runs AG.

---

#### References:

This Advisory and Upcoming Advisories:  
[http://www.nruns.com/security\\_advisory.php](http://www.nruns.com/security_advisory.php)

---

#### About n.runs:

n.runs AG is a vendor-independent consulting company specialising in the areas of: IT Infrastructure, IT Security and IT Business Consulting.

#### Copyright Notice:

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact [security@nruns.com](mailto:security@nruns.com) for permission. Use of the advisory constitutes acceptance for use in an "as is" condition. All warranties are excluded. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Copyright 2010 n.runs AG. All rights reserved. Terms of use apply.