

Vendor: Alcatel  
 Affected Products: OmniVista 4760 server: all versions prior to  
 release R5.1.06.03.c\_Patch3.  
 Vulnerability: arbitrary code execution  
 Risk: High  
 CVE-Number: CVE-2010-3281

## 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 and that n.runs initially found the bug in 2006 during a  
 customer project and the customer has been trying from then until  
 the beginning of 2010 to get the issue fixed. Customer has  
 requested from n.runs to take over the handling of vulnerability  
 and to publish it.  
 2010/02/24 confirmation from Alcatel-Lucent that the vulnerability exists  
 2010/03/15 n.runs confirms CVSS rating  
 2010/08/10 Alcatel-Lucent confirms that vulnerability is fixed  
 (fix date: 2010/05/06)  
 2010/08/23 Alcatel-Lucent proposes September 15th as the publication date  
 and requests a CVE number  
 2010/09/13 Business Partners of Alcatel-Lucent are informed about the  
 vulnerability  
 2010/09/15 CVE number received  
 2010/09/20 n.runs AG releases this advisory

## Overview:

-----  
 Part of the Alcatel Omnivista 4760 administration software of the Alcatel  
 4400 PBX is an HTTP proxy. It is used to tunnel ssh-connections to the ssh-ports  
 of the PBX within the internal network.  
 This proxy is vulnerable to a remote buffer overflow.

## Description:

-----  
 By sending a long HTTP GET request it is possible to overwrite CPU registers.  
 Due to this vulnerability, an attacker can control the execution path remotely.

## Impact:

-----  
 Arbitrary code can be executed on the proxy server from remote.  
 On a normal setup the HTTP proxy is running on the same machine as the 4760  
 management system.  
 Due to this vulnerability an attacker can gain access to administrative  
 functions of the PBX and to the internal network, possibly a DMZ.

## Solution

-----  
Mitigation

Protect the HTTP proxy function on the 4760 server with the windows internal  
 firewall by restricting access to workstations with a known pre-declared  
 IP address:

In the windows firewall configuration, for the exception concerning the 4760  
 Communication Server, modify the extent of allowed systems by removing the  
 authorization for any IP system with the precise list of the specifically  
 allowed IP addresses.

Note: include the 4760 server own address in this list to enable the embedded  
 4760 client as well.

## Fixed Software Versions/Patches and how to obtain them

Omnivista 4760 version R5.1: install the Patch3 for version 5.1.06.03.c\_Patch2  
 (or the full delivery 5.1.06.03.c\_Patch3 when it is available).  
 Omnivista 4760 version R5.0 and prior: upgrade to Omnivista 4760 version R5.1

and installation of patch is recommended.

---

Credits:

Bug found by Axel Rengstorf of Bluebox Security, Dirk Breiden 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.