

## Remote Execution Vulnerability in OmniPCX Office

### Summary

A vulnerability has been discovered in OmniPCX Office with Internet Access services, allowing an attacker on Internet to potentially access OXO resources.

### Risk analysis

CVSS Score : 7.31

CVSS Base Score	x	CVSS Temporal Score	Y	CVSS Environmental Score	z
Access Vector	0.65	Exploitability		Collateral Damage Potential	
Access Complexity	0.71	Remediation level		Target distribution	
Authentication	0.70	Report confidence			
Confidentiality impact	0.28				
Integrity impact	0.25				
Availability impact	0.66				
Impact bias					

### Affected Products and Configurations

OmniPCX Office since release 210/061.1

### Non-Affected Products and Configurations

### Detailed vulnerability description

A CGI scripts used by OmniPCX Office with Internet Access services does not correctly filter some specific parameters. As a consequence, some sensitive information can be retrieved from Internet.

### Impact of the vulnerability

Sensitive information can be disclosed and control of the system may be gained.

### Solutions

#### Workaround

The workaround consists in preventing WBM/WCA access from Internet.

From R2.1 towards R4.1:

- Sign-in WBM with admin account



- Go to the "Firewall" configuration screen
- Select the "Firewall Settings" URL
- Select the "Services" tab
- Unselect the "Web-Based Management (WBM)"
- Unselect the "Web-Communication Assistant"
- Apply the modifications
- Sign-out

From R5.1 towards R6.1:

- Sign-in WBM with admin account
- Go to the "Firewall" configuration screen
- Select the "Firewall Settings" URL
- Select the "HTTP/HTTPS" tab
- Unselect the "HTTPS services" ("Services available from WAN network using HTTPS")
- Unselect the "HTTP services" ("Services available from WAN network using HTTP")
- Apply the modifications
- Sign-out

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

OX0210: upgrade to release 210/091.001

OX0310: upgrade to release 310/056.001

OX0410: upgrade to release 410/057.001

OX0510: upgrade to release 510/037.001

OX0600: upgrade to release 610/014.001

### References

Reporter reference : DSECRG-08-020

Internal reference number : SA034

CVE entry number : 2008-1331

Cert-IST reference number : CERT-IST/AV-2008.151

### History

Date of vulnerability notification : january 8<sup>th</sup>, 2008

Date of informing customers or business partners : march 7<sup>th</sup>, 2008

Date of document publishing on our external PSIRT website : april 1<sup>st</sup>, 2008

### Acknowledgements

Alcatel-Lucent would like to thank Digital Security (<http://dsec.ru>) to inform us about this vulnerability, for the good cooperation and for acting according to our disclosure policy practices. We encourage others to report any potential vulnerabilities by sending a Vulnerability Summary Report to [psirt.security@alcatel-lucent.com](mailto:psirt.security@alcatel-lucent.com). As such we will be able to improve the security characteristics of our products and the environments in which they are deployed.



## Vendor Statement

ALU is committed to continuously enhancing our security posture, and we have both internal and external resources involved in security review processes aimed at identifying product vulnerabilities, both in existing and in developing products.

It is important to note that there have been no reports of compromise due to this vulnerability. ALU's primary concern in this instance is to rapidly deploy a solution for our entire customer base. As a result, ALU has released patches for most code versions.

We highly recommend that you upgrade your products to a patch corresponding to your currently installed release. While we encourage customers to always utilize the latest releases to ensure the full benefit of our continued innovation and improvements, we recognize that this is not always possible.

Information on our disclosure policy, how to report vulnerabilities and a list of public advisories can be found at our PSIRT website : <http://www1.alcatel-lucent.com/psirt>