

Cross-site scripting vulnerabilities in OmniVista 4760

Summary

Two cross-site scripting vulnerabilities have been discovered in OmniVista 4760.

CVSS Score (base metrics only):

CVSS Base score	5.2
Access Vector	Remote
Access Complexity	Low
Authentication	Not required
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	None
Impact Bias	Weight confidentiality

History

Date of notification: June 20, 2007

Date of publication: Ed.01 (October 15, 2007)

Affected Products and Configurations

OmniVista 4760 version R4.2 and prior, when accessing the Web Directory application through a Web browser.

Detailed description

The OmniVista 4760 home page gives access to 2 applications through a Web browser: the Web Directory application and the Network configuration application. Only the 4760 home page and the Web Directory application are affected, the Network configuration application is not.

Access through a Web browser is mandatory for any of these vulnerabilities to be exploited. The user has to click on a crafted URL, either received through email or retrieved from bookmark lists.

The first vulnerability allows HTML code to be injected in the OmniVista 4760 home page.

The second vulnerability allows JavaScript code injection in the Web Directory application.

Impact of these vulnerabilities

None of these vulnerabilities affect the full weight 4760 client application installed on client workstations. The Network configuration application is not impacted.

The first vulnerability enables an attacker to alter the display of the 4760 home page.

The second vulnerability allows an attacker to run arbitrary JavaScript code under the identity of the user accessing the crafted URL in the context of its Web browser, potentially resulting in confidential information disclosure like cookies or local file alteration or destruction.

For more information on cross-site scripting vulnerabilities and their impacts, see this Wikipedia article: http://en.wikipedia.org/wiki/Cross-site_scripting.



Solutions

Workaround

Use the full weight OmniVista 4760 client application.

If use of a Web browser is mandatory:

- directly enter the URL of the OmniVista 4760 home page in the navigation toolbar (against the first vulnerability);
- access the Web Directory application only from the OmniVista 4760 home page (against the second vulnerability).

Never access the OmniVista 4760 home page or the Web Directory application through bookmarks, URLs received through email or found on unsafe Web sites.

For more information on avoiding cross-site scripting vulnerabilities, see this Microsoft support article: “Preventing Internet Explorer and Outlook Express Cross-Site Scripting Security Issues” at <http://support.microsoft.com/kb/253117>.

Fixed Software Versions and how to obtain them

OmniVista 4760 version R4.2: install the patch called “PatchL_php.ace” for version 4.2.0.6.

OmniVista 4760 version R4.1 and prior: upgrade to OmniVista 4760 version R4.2 is recommended.

References

Discoverer reference: S21sec (<http://www.s21sec.com/>)

CVE entry number: CVE-2007-5190

CERT-IST/AV-2007.475 « Cross-site scripting vulnerabilities in OmniVista 4760 »

This vulnerability is tracked as Alcatel-Lucent defect number XTScf01120.

Vendor Statement

Alcatel-Lucent 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. Alcatel-Lucent’s primary concern in this instance is to rapidly deploy a solution for our entire customer base. As a result, Alcatel-Lucent has released a patch for the most recent code versions and offers customers with an earlier release a free upgrade to that version.

We highly recommend that you upgrade your OmniVista 4760 to version R4.2 with the corrective. While we encourage customers to always utilize the latest release 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 can be found at <http://www1.alcatel-lucent.com/psirt>.