Security Research Advisory

Genesys Voice Portal Manager
Cross-Site Scripting Vulnerability

Table of Contents

Cross-Site Scripting (XSS)					Advisory Number
					SN-08-03
Severity	Software	Version(s)	Accessibility	CVE	Author(s)
M	Voice Portal Manager	7.2.015.02	Remote	-	Claudio Criscione
	Vendor URL		Advisory URL		
	www.genesyslab.com		-		

Date	Details
28/05/2008	Vendor disclosure
-	Vendor acknowledgment
-	Patch release
01/07/2008	Public disclosure

Summary

Genesys is a leading company in providing VOIP solutions, and, according to its website, the world's first contact center software company.

Voice Portal Manager is part of Genesys Voice Platform, a software standards-based platform that enables businesses to provide cost-effective customer interactions 24x7.

Genesys Voice Platform provides touchtone access to applications and incorporates speech recognition technology for conversational exchange to identify and resolve customer requests.

Voice Portal Manager's web console is prone to Cross-Site Scripting vulnerability due to lack of input sanitization.

Vulnerability Details

Secure Network discovered an input validation error which leads to an XSS vulnerability in Voice Portal Manager's web console. The *dynamicTreeXSL* parameter is not validated before being printed in the *content_with_frame.php* page.

The vulnerability was discovered and tested on version 7.2.015.02, but other versions are likely to be vulnerable as well.

Technical Details

Description

A PoC is provided below.

PoC URL:

```
/content_with_frame.php?service=IPCS&dynamicTreeXSL="></iframe><script>alert('SNXSS')</script>XSS&action=IPCSSummary&title=IPCS%20Call%20Summary&nodePath=
```

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41