

CSS09-01: SlideShowPro Director File Disclosure Vulnerability

August 6, 2009

SUMMARY

SlideShowPro Director is vulnerable to a file disclosure flaw because it fails to perform proper validation and handling of input parameters. Attackers can exploit this vulnerability to read arbitrary files from the hosting web server.

AFFECTED SOFTWARE

SlideShowPro Director version 1.1 through 1.3.8.

SEVERITY RATING

Rating: High Risk

Impact: Unauthorized access to system files

Where: Remote

SOFTWARE DESCRIPTION

SlideShowPro Director is a complement to SlideShowPro, “a web-based component designed to be integrated into any web site ... for displaying photos and videos.” Director is “a secure, easy to use application you install on your own web server...for managing and updating your slideshow content...”

Link: http://slideshowpro.net/products/slideshowpro_director/slideshowpro_director

SOLUTION

The vendor has released version 1.3.9 to address this issue. Refer to <http://wiki.slideshowpro.net/SSPdir/UP-HowToUpgrade> for upgrade instructions.

REFERENCES:

CVE number not yet assigned.

TECHNICAL DETAILS

The “p.php” file contains logic that is vulnerable to directory traversal attacks. The “a” parameter to this function includes a file name parameter that can be changed to any value, including one containing relative directory paths. The resulting file will be retrieved and displayed.

The application incorporates scrambling/obfuscation techniques to mask the vulnerable parameter that is supplied to the application. A moderately skilled attacker can reverse the obfuscation without any access to the affected server or source code.

IDENTIFYING VULNERABLE INSTALLATIONS

Vulnerable installations can be identified by the XML data file generated by SlideShowPro Director and used by the SlideShowPro component and will have base64-encoded “a” parameters to the “p.php” function:

```
<?xml version="1.0" encoding="utf-8"?>
<!-- XML Generated by SlideShowPro Director v1.3.8
http://www.slideshowpro.net -->
<gallery title="masked" description="masked">
  <album id="album-17" title="masked" description=""
lgPath="http://masked/ssp_director/p.php?a="
tnPath="http://masked/ssp_director/p.php?a="
tn="http://masked/ssp_director/p.php?a=XF9VXiEyPSoqQFtFPzU2JzM6Iys%2BPiYyKzM5
LTM%2BMiU%2BJzE%3D&am;p;m=1247688172">
```

DETECTING EXPLOITATION

The affected parameter is only accepted as a “GET” variable. The web server should therefore log any exploitation attempts if basic logging is enabled. Identifying actual exploitation is hindered, since the attacking parameter is scrambled, but the logic to reverse this data can be extracted the application code and settings if necessary. Web server error logs may also contain suspicious PHP file access warnings if a file requested by an attacker is not present.

PROOF OF CONCEPT

A proof-of-concept tool to exploit this vulnerability that accommodates the parameter scrambling for any site has been created but not published. Note that even sites that have defined a custom “key” or “salt” for the scrambling routines are vulnerable.

IMPACT

This issue exposes the confidentiality of any files residing on the same drive as the component including configuration files with system access credentials, the source code to application pages, and possibly customer data files.

THREAT EVALUATION

The issue can be exploited by anyone from the Internet. The ability to identify/crack the scrambling key would require a moderately skilled individual, although once the algorithm is published, exploiting the issue is trivial. This vulnerability can be easily scripted and automated, placing it within reach of any individual. An attacker must know the name of desired files.

CREDITS

Scott Miles of Clear Skies Security identified this flaw.

Clear Skies would like to thank the vendor for their openness and responsiveness in dealing with this issue.

TIME TABLE

2009-07-20 – Vendor notified; confirmed vulnerability.

2009-07-22 – Vendor provides patch.

2009-08-06 – Public disclosure.