Path Injection in EyeOS development trunk

Title: Path Injection in EyeOS development trunk
Release Date: 2013/03/01
Vulnerable Application: EyeOS development trunk
Type: Path injection
Level: Very High (Low/High/Critical)
CVSS: 6.3 (Av:N/AC:L/Au:N/C:P/I:P/A:P)

Dognædis Ref.: DGS-SEC-13
CVE Ref.: CVE-2013-2284
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): DMarcos - CodeV Team
Contact: irt@dognaedis.com

Overview:

EyeOS invented the web desktop 6 years ago and it is today the leading Cloud Desktop worldwide. Headquartered in Barcelona, EyeOS is one of the biggest Open Source projects in Europe with more than 1 million downloads and communities across the globe.

IBM has selected EyeOS as its preferred Open Source Cloud platform in 2010 and signed a global partnership. Gartner named EyeOS Cool Vendor in IT Operations management in 2011. The company has closed its first funding round with Spanish VCs and Business Angels in June 2011 and has just launched in October 2011 its first commercial license, the EyeOS Professional Edition.

Scope:

File: <app_root>/devtools/qooxdoo-sdk/framework/source/resource/qx/test/part/delay.php[7:24]
Vulnerable Argument(s): $_GET['file']
Code:

```
line 20: echo file_get_contents($_GET['file']);
```

Proof(s) of Concept:

```
<app_root>/devtools/qooxdoosdk/framework/source/resource/qx/test/part/delay.php?file=../../../../../../../../../../../../../../../etc/passwd
```

Description:

The referred vulnerabilities could be exploited through Path Injection attacks, aiming to search content from the server that is not accessible by the user. It could also be used to search content from files outside of the server document root. Despite existing some ".htaccess" files to avoid the direct calling of the referred files, the "AllowOverride" directive is, in most cases, set to "None" by default in the Apache configuration, making this protection uneffective.

Impact:

The server may show content from files that are not supposed to be access by the user, representing a probable confidentiality breach. That can put integrity and server availability at risk.

Resolution:

The path should be validated against application and user boundaries.

Official Solution:

At the moment, there is no official solution for the reported vulnerabilities.

External References:

https://www.owasp.org/index.php/Relative_Path_Traversal
https://www.owasp.org/index.php/Path_Traversal
https://www.owasp.org/index.php/Resource_Injection