

MWR InfoSecurity Security
Advisory

Elastic Path Arbitrary File
System Access (Multiple
Vulnerabilities)

22nd February 2008



Contents

1	Introduction	5
2	Arbitrary File Download.....	5
2.1	Technical Background.....	5
2.2	Vulnerability Details.....	5
2.3	Exploit Information	5
3	Arbitrary File Upload.....	6
3.1	Technical Background.....	6
3.2	Vulnerability Details.....	6
3.3	Exploit Information	6
4	File System Browse.....	7
4.1	Technical Background.....	7
4.2	Vulnerability Details.....	7
4.3	Exploit Information	7
5	Dependencies.....	8
6	Recommendations.....	9

Elastic Path Arbitrary File System Access Vulnerabilities

Package Name:	Elastic Path
Date:	22 nd November 2007
Affected Versions:	4.1 and 4.1.1

CVE Reference	Not Yet Assigned.
Author	Daniel Martin Gomez
Severity	High.
Local/Remote	Remote.
Vulnerability Class	Arbitrary file download, file upload and file system browsing through directory traversal.
Vendor URL	http://www.elasticpath.com/
Version	4.1 and 4.1.1
Vendor Response	A patch has been developed for Elastic Path versions 4.1 and 4.1.1.
Exploit Details Included	Yes, although no exploit code is included in this advisory.
Affected OS	The vulnerabilities have been confirmed on Windows Server 2003; however, all platforms are expected to be affected.

Overview:

Multiple input validation vulnerabilities were identified within the Elastic Path application. As a result, directory traversal is possible and this allows unrestricted file system access (browse/upload/download) to the remote server, depending on the read/write privileges of the user account.

Impact

An attacker could display the contents of the server's file system. In addition to this, the vulnerabilities would enable both the upload and download of files to and from arbitrary locations on the affected system.

Cause

Multiple input validation routines fail to adequately validate file system related parameters making directory traversal possible.

Interim Workaround

Introduce host based or network filtering controls to restrict access to the affected service such that it can only be accessed from authorised IP addresses. Application users should be granted the lowest level of privilege consistent with their required tasks.

Solution

The vendor has developed a patch to address these vulnerabilities in Elastic Path versions 4.1 and 4.1.1. Currently, this has not been tested by MWR InfoSecurity.

To obtain the patch users must contact the vendor at support@elasticpath.com or <http://www.elasticpath.com/support/>.

1 Introduction

Elastic Path is a popular Java e-commerce software platform for building online stores and shopping carts. Elastic Path consists of both a shopping front end which allows customers to browse and choose products, and the Elastic Path Commerce Manager for administrative purposes. This includes features such as a search engine, merchandising, customer management, order management, etc.

Users of the administrative interface can be granted different levels of access. Research revealed that users with upload/download privileges could abuse them to gain access to arbitrary files on the remote system.

2 Arbitrary File Download

2.1 Technical Background

In this instance, the directory traversal is possible because of insufficient validation of user supplied input file names. Characters representing the command 'traverse to parent directory' can be passed through to the file system functions of the underlying programming language.

This attack uses the application to access computer files which are not intended to be accessible.

2.2 Vulnerability Details

The directory traversal vulnerability was present in the script used by the application when a user requested the download of a file.

Insufficient validation in the **file** parameter could enable an attacker to download arbitrary files from the remote system.

2.3 Exploit Information

In order to exploit this vulnerability an attacker would need to determine the actual path in which the Elastic Path application is deployed. However, this is easily achieved by generating an error message such as the one returned after issuing an invalid request:-

```
https://www.domain.com/elasticpath_dir/manager/reportDetail.jsp?file=c:\\boot.ini
```

Once this location is known, the file parameter of the **getImportFileRedirect.jsp** script can be used to access arbitrary files:-

```
https://www.domain.com/elasticpath_dir/manager/getImportFileRedirect.jsp?type=mapping  
&file=../../../../../../../../boot.ini
```

3 Arbitrary File Upload

3.1 Technical Background

A similar input validation flaw allows files to be uploaded to arbitrary locations.

Whenever a user is allowed to upload files to a server a potential security risk is created. If the input validation routines that handle these requests are not sufficiently strong then malicious files can be uploaded and executed under the context of the application server.

3.2 Vulnerability Details

The script used by the application to handle upload file requests was found to apply insufficient validation to user input. As a result, an attacker could use the `importData.jsp` file to upload arbitrary files to arbitrary locations on the remote web server.

An attacker could exploit this vulnerability to upload malicious files to the server such as back doors or Trojan horses which could be used to further compromise the system.

3.3 Exploit Information

Investigation revealed that the input validation function used to handle the file name was of the following form:-

```
String s = uploaded_file_name //from the web form
if (s.indexOf("/") > 0 )
    return s.substring(s.lastIndexOf("/") + 1, s.length());
else
    return s.substring(s.lastIndexOf("\\") + 1, s.length());
```

However, this validation routine can be bypassed by supplying a specially crafted file name for the uploaded file. An example of this is given below:-

```
../../../../..\Browser.jsp
```

Using this technique (and having determined the actual path in which the server content is located), it would be possible to store a malicious file in the document root of the web server.

Depending on the privileges under which the server is running this vulnerability could be exploited to overwrite system files and install malware on the remote system. It could also be used to upload a malicious file which could then be used to execute commands under the server context.

4 File System Browse

4.1 Technical Background

A further input validation flaw gives rise to a directory traversal vulnerability which results in the ability to browse or display the contents of arbitrary folders on the server file system.

4.2 Vulnerability Details

This is the easiest vulnerability of the three to exploit. The application provides a script to manage the resource files associated with shop products, **fileManager.jsp**. Inspection of the source code of this script revealed that insufficient validation in the **dir** parameter could allow an attacker browse through the contents of arbitrary locations on the remote drive.

4.3 Exploit Information

An example query which exploits this vulnerability is given below:-

```
https://www.domain.com/elasticpath_dir/manager/fileManager.jsp?dir=../../../../WINDOWS/system32/config/
```

5 Dependencies

Exploitation of all the vulnerabilities described above requires a request to be made to the web server. Therefore, network filtering could be used to mitigate these risks. However, it is acknowledged that as web servers are designed to be publicly accessible this will not be practical in the majority of circumstances.

Successful exploitation of these attack vectors requires the attacker to be logged onto the Elastic Path Commerce Manager. In addition to this, the logged in user would need download or upload rights to exploit the arbitrary file download and upload vulnerabilities.

6 Recommendations

The vendor has developed a patch to address these vulnerabilities in Elastic Path versions 4.1 and 4.1.1. Currently, this has not been tested by MWR InfoSecurity.

To obtain the patch users must contact the vendor at support@elasticpath.com or <http://www.elasticpath.com/support/>.

To reduce the level of risk to which users of the software are exposed it is further advised that the server hosting the application be run under a system user account with the lowest level of privilege possible.

It is also recommended that, where possible, the Elastic Path Commerce Manager should be subject to network level filtering such that only trusted IP addresses can communicate with the service. It should be noted that this is a generic recommendation and is not specific to this technology.

MWR InfoSecurity
St. Clement House
1-3 Alencon Link
Basingstoke, RG21 7SB
Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083
mwrinfosecurity.com