

# Patching Spip for forum.php3 vulnerability

**Baptiste SIMON (aka BeTa)**  
e-glop.net

This document aims to give the keys for lambda users to upgrade their Spip-1.4.2, Spip-1.5.2 or Spip-1.6 to a patched fully-compatible version. The files on which we work on can be found at [ <http://www.e-glop.net/dev/spip/> ]

## 1. Files description

<http://www.e-glop.net/dev/spip/SPIP-v1-4-3.patch.gz>

Patch to upgrade from SPIP-v1.4.2 to SPIP-v1.4.3

<http://www.e-glop.net/dev/spip/SPIP-v1-4-3.inc-forum.php3.gz>

Patched file to replace in SPIP-v1.4.2 to upgrade to SPIP-v1.4.3

<http://www.e-glop.net/dev/spip/SPIP-v1-5-3.patch.gz> (<http://www.e-glop.net/dev/spip/SPIP-v1-5-3.patch.gz>)

Patch to upgrade from SPIP-v1.5.2 to SPIP-v1.5.3

<http://www.e-glop.net/dev/spip/SPIP-v1-5-3.inc-forum.php3.gz>

Patched file to replace in SPIP-v1.5.2 to upgrade to SPIP-v1.5.3

<http://www.e-glop.net/dev/spip/SPIP-v1-6-1.patch.gz>

Patch to upgrade from SPIP-v1.6 to SPIP-v1.6.1

<http://www.e-glop.net/dev/spip/SPIP-v1-6-1.inc-forum.php3.gz>

Patched file to replace in SPIP-v1.6 to upgrade to SPIP-v1.6.1

<http://www.e-glop.net/dev/spip/spip-cert.txt>

The official security announce

[http://www.e-glop.net/dev/spip/upgrading.\\*](http://www.e-glop.net/dev/spip/upgrading.*)

This "howto" in different formats.

## 2. Upgrading from patch (the *regular* and preferred choice)

### 2.1. Needs

You need :

- a shell access to your website's sources,
- the "patch" package installed. You can certainly find it in your distribution's packages manager as "patch". In anyway, this is the official *\*patch\** website (<http://www.gnu.org/software/patch/patch.html>),
- the "gzip" package installed. You can certainly find it in your distribution's packages manager as "gzip". In anyway, *this is the official \*gzip\* website*,
- the "wget" package is also recommended. You can certainly find it in your distribution's packages manager as "wget". In anyway, *this is the official \*wget\* website*.

### 2.2. Proceeding...

That is the way to patch your website's sources

```
$ cd /path/to/your/spip/dir
$ wget http://www.e-glop.net/dev/spip/SPIP-v1-5-3.patch.gz (or whatever version you are running)
$ zcat SPIP-v1-5-3.patch.gz | patch -p1
```

Replace the name 'SPIP-v1-5-3.patch.gz' with the patch version you need for your current Spip website.

## 3. Upgrading without patching

### 3.1. Needs

Duplicate implicit target name: "needs".

You need

- to be able to gunzip the files. If you're running any UNIX, try to find the gunzip command. If you don't find it, try to install it the way you use to do. The gunzip command can be found in the gzip package (<http://www.gnu.org/software/gzip/gzip.html>).
- the "wget" package is also recommended. You can certainly find it in your distribution's packages manager as "wget". In anyway, *this is the official \*wget\* website*. If you are not using wget (because you prefer another software or because you're running the Microsoft OS), replace the wget command line by the software you prefer.

## **3.2. Proceeding...**

Duplicate implicit target name: "proceeding...".

To replace the vulnerable script in your website's sources, please download the pre-pathed file corresponding to your Spip version. The patched files can be found at URL like :  
'<http://www.e-glop.net/dev/spip/SPIP-v1-5-3.inc-forum.php3.gz>'. To find the file you need, please refer to the files listed at the top of this document.

Once you've got it, gunzip it and replace your website's 'inc-forum.php3' file with this one.

Here is a script example for UNIX users

```
$ cd /path/to/your/spip/dir
$ wget http://www.e-glop.net/dev/spip/SPIP-v1-5-3.inc-forum.php3.gz (or whatever version you are
$ gunzip SPIP-v1-5-3.inc-forum.php3.gz
$ mv -f SPIP-v1-5-3.inc-forum.php3 inc-forum.php3
```

## **4. And...**

That's done !

Please verify if your website is protected against the forum.php3 vulnerability by trying to reproduce the scenario described in the cert© document that you can find here (<http://www.e-glop.net/dev/spip/spip-cert.txt>).

If your website is still vulnerable, please retry patching once again, and then, contact me ([mailto:bs-public\\_NOSPAM\\_e-glop.net](mailto:bs-public_NOSPAM_e-glop.net)) and the spip development team ([mailto:spip-dev\\_NOSPAM\\_rezo.net](mailto:spip-dev_NOSPAM_rezo.net)) to report your problem.

## **5. Annexes**

### **5.1. The author**

Baptiste SIMON (<http://www.e-glop.net/>) <[baptiste.simon @ e-glop.net](mailto:baptiste.simon@e-glop.net)  
([mailto:baptiste.simon\\_NOSPAM\\_e-glop.net](mailto:baptiste.simon_NOSPAM_e-glop.net))>

Administrateur système GNU/Linux & UNIX

In the search of an employment (<http://www.e-glop.net/cv/>)

## **5.2. This document other formats**

This document has been written in RST (<http://docutils.sourceforge.net/>) with KWrite and then converted into DN-XML and Docbook with dn2dbk.xml (<http://membres.lycos.fr/ebellot/dn2dbk/>).

The XHTML, HTML and XSL-FO versions have been created with the official DocBook XSLT stylesheet <sup>1</sup>. The PDF, Postscript, RTF and plain text versions have been create with Jade (<http://openjade.sourceforge.net/>).

Find all those formats here :

- XHTML (<http://www.e-glop.net/dev/spip/upgrading.xhtml>)
- HTML (<http://www.e-glop.net/dev/spip/upgrading.html>)
- PDF (<http://www.e-glop.net/dev/spip/upgrading.pdf>)
- postscript (<http://www.e-glop.net/dev/spip/upgrading.ps>)
- Texte brut (<http://www.e-glop.net/dev/spip/upgrading.txt>)
- RTF (<http://www.e-glop.net/dev/spip/upgrading.rtf>)
- reStructuredText (<http://www.e-glop.net/dev/spip/upgrading.rst>)
- DocBook - XML (<http://www.e-glop.net/dev/spip/upgrading.db-xml>)
- DN-XML (<http://www.e-glop.net/dev/spip/upgrading.dn-xml>)
- XSL-FO (<http://www.e-glop.net/dev/spip/upgrading.fo>)

## **5.3. Publication License**

This document from [www.e-glop.net](http://www.e-glop.net) (<http://www.e-glop.net/>) is published under the Open Publication License (<http://www.opencontent.org/openpub/>). Permission is granted to copy, distribute and/or modify this document under the terms of the Open Publication License (<http://www.opencontent.org/openpub/>) version 1.0.

## **Notes**

1. The app-text/docbook-xsl-stylesheets (<http://www.oasis-open.org/docbook>) package on Gentoo-Linux