Legacy Deltik Products

Deltik, Monday 19 September 2016 - 01:32:46

In the past, Deltik's products site, products.deltik.org, provided demos of the products published by Deltik from 2008 to 2011. Some of these products have serious security or performance flaws that made them unsuitable for demoing on Deltik.

As a result, the old products, now collectively called the "Legacy Deltik Products", have been taken off of the demo site and published as an unsupported archive.

Installation

The Legacy Deltik Products can be copied to any web server running PHP 5, and they should run roughly as they did on Deltik. Note that some paths were hard-coded and may break on your web server if you aren't pretending to use the virtual host products.deltik.org.

You can find the products on the Legacy Deltik Products GitHub repo and clone them with this command:

```
git clone https://github.com/Deltik/products-legacy.git
```

A .tar.xz archive containing only the products folder can be downloaded directly from GitHub or from Deltik.

Either of these commands performs the download and extraction into the current directory:

```
curl -L 'https://github.com/Deltik/products-legacy/raw/master/products.tar.xz' | tar -xJvf -
```

```
curl -L 'https://content.deltik.net/products/legacy/products.tar.xz' | tar -xJvf -
```

What's Included

The GitHub repo contains a README.md file that explains what's included.

What's Happening to products.deltik.org

Currently, https://products.deltik.org/ just contains a static page explaining what happened to the Legacy Deltik Products. If I choose to make something of the subdomain, I'll replace it with whatever succeeds the Legacy Deltik Products.

Problems with the Demos

The demos ran on the same unprivileged user as the main Deltik website, which means that compromising one of the demos would allow an attacker to take control of Deltik. I provide an example of a partial exploit in the extended version of this news post. (I figured that it would be pointless to demonstrate a full exploit, since the demos are no longer running here.)

It was also possible to do some denial of service attacks and proxy some attacks through this server. I present a high-level overview of some attack examples in the extended version of this news post.

[html]
Security
Kweshuner
Kweshuner had a really useful feature that let you display the contents of any file accessible to the site's unprivileged user, including my emails and the configuration file that contains the database password to this website. To get the database password, all you had to do was go to this URL:

https://products.deltik.net/kweshuner/kweshuner_old/?page=admindebug&file=/home/deltik/public_html/e107_config.php

The code that made this laughably easy was line 470 of products/kweshuner/kweshuner_old/index.php.

Deltik Products Portal
The portal itself at https://products.deltik.net/ was vulnerable to SQL injection because SQL inputs were not sanitized. This was the vulnerable string:

```
"SELECT * FROM `nodes` WHERE `id` = ".$_REQUEST['id']
```

And the URL in which you could put an injection was:

https://products.deltik.net/?action=status&id=YOUR_INJECTION_HERE

Even though the script was expecting an integer value, the input wasn't even cast as int. See line 31 of core.php.

Performance
MuSeSPinger
It is easy to conduct a denial of service attack on MuSeSPinger by specifying many slow hosts to check and repeatedly requesting them until the hosting account running MuSeSPinger exhausts its resources. Generated images are not cached and take as long to respond as the slowest host checked.

Log2Log PHP The implementation is very CPU- and RAM-intensive. It loads up all provided chat logs into RAM and keeps eating up RAM during the conversion process. The conversion process takes up a lot of time and makes the server busy, as can be seen in this earlier blog post. I really should have written a proper apology for the rampant abuse caused by Log2Log PHP, but it's been over five years. Matt, if you're reading this, I'm sorry. [/html]html