Press Release

Reflected XSS in Typo3 Formhandler

softScheck has identified a Reflected Cross-Site-Scripting (XSS) vulnerability in the Typo3 extension "Formhandler" through manual code review. An attacker can pass a hidden form parameter which is reflected without validation, even if the form does not make use of it. The vulnerability results in JavaScript code execution in the victim's browser.

Product: Typo3 Formhandler (http://www.typo3-formhandler.com/)

Affected Versions: 2.3.0 and below

CVE: (requested)

CVSS: 6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Description: A reflected XSS vulnerability was identified in the formToken parameter in Classes/View/Form.php, line 483:

```
<input type="hidden" name="' . $name . '" value="' . $this->gp['formToken'] . '" />
```

The variable "formToken", which can be passed via GET or POST, is reflected unfiltered in the HTML output. Formhandler applies some additional XSS mitigation in Filtreatment.php, however it can be circumvented.

Proof of Concept: The following Proof of Concept creates a link "Click here!" in the contact[formToken] parameter that contains base64-encoded JavaScript. Once clicked, it executes an "alert('xss')". The parameters contact[message] and contact[randomID] are left empty to provoke an error such that the partially filled out form is reflected back at the user.

```
http://examples.typo3-formhandler.com/basic-forms/contact-
form/?id=290&contact[submitted]=1&contact[randomID]=&contact[removeFile]=%0D&contac
t[removeFileField]=%0D&contact[submitField]=%0D&contact[step-2-
next]=1&contact[name]=x&contact[email]=x@y.z&contact[message]=&contact[step-2-
next]=Send&contact[formToken]="></fieldset><h1><a
href="data:text/html;base64,PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4=">Click%20here!
</a></h1><br
```

Remediation: Update Formhandler to version 2.3.1 or 2.0.2, respectively.

Timeline:

2016-04-12: Report to extension author Reinhard Führicht

2016-04-12: Author acknowledges vulnerability, reports to security@typo3.org

2016-05-17: Report to security@typo3.org

2016-05-27: Patch released, versions bumped to 2.3.1 and 2.0.2. Typo3 releases Security Bulletin: https://typo3.org/teams/security/security-bulletins/typo3-extensions/typo3-ext-sa-2016-011/

2016-05-31: CVE ID requested

About softScheck:

Starting life in 2001 as a world leading Information Security Institute, softScheck evolved into an IT security company, offering its clients the highest level of product penetration testing. With over a decade of experience, our clients benefit from state of the art security testing developed by renowned research experts. Our methods and technology form the cutting edge of IT security, with our staff comprising of leading researchers and academics.

Contact:

Mahtab Delschad
Tel.: +49 2241 – 255 43 – 0
Fax: +49 2241 – 255 43 – 29
mahtab.delschad@softScheck.com

softScheck GmbH
Bonner Straße 108
53757 Sankt Augustin
www.softScheck.com