☰

CVE 2020-6171 – Cross-Site Scripting in CLink Office v2

During the conduct of a threat assessment for a major Fortune 500 (https://www.deepcode.ca/index.php/portfolio/project-threat-assessment/) company, DeepCode (https://www.deepcode.ca/) analyzed web-based targets hosted on a Hong-Kong based company named *CommuniLink* (https://www.communilink.net/). Customers can manage back-office services such as mail and spam configuration via a control panel called *CLink Office*, which is made by *CommuniLink* itself. This application is vulnerable to at least one Cross-Site Scripting (https://owasp.org/www-community/attacks/xss/) (XSS) via parameter injection. As of 18 January 2020, a simple Google search (https://www.google.com/search?q="CLink+Office+v2") returned 2,500 web servers using the application, mostly in Hong Kong.

> "CLink Office v2"
>
> 🔍 All   🖼 Images   🔍 Shopping
>
> About 2,540 results (0.38 seconds)

The CLink Office v2 Control Panel is believed to be used by 2,500 hosts, mostly located in Hong Kong.

Security Issues

The control panel has multiple issues. The first being that it uses a vulnerable version of the Horde webmail (https://www.horde.org/apps/webmail)client. Despite commenting out the link on the main page, the developer left the actual web application on the clients' hosts.

Commented code in the CLInk Office v2 Control Panel, leading the a vulnerable Horde IMP (https://www.horde.org/apps/imp) application.

From there, an adversary can access the Horde login page via the `/horde/imp/login.php` link, which is opened to various vulnerabilities (https://www.cvedetails.com/product/1021/Horde-IMP.html?vendor_id=593), including Local File Inclusion (LFI) and Remote Code Execution (RCE) vulnerabilities.

LFI vulnerability (https://www.exploit-db.com/exploits/16154) in the "hidden" Horde IMP page is still functional.

Cross-Site Scripting in the *lang* Parameter

The application uses the *lang* parameter to display the page in English or Chinese, however, the content of the parameter is not filtered, allowing the injection of HTML/JavaScript code. The PoC of this vulnerability is included below:

```
http://example.com/?
lang=%22%3E%3Cscript%3Ealert(%27xss%27)%3C/script%3E%3Cp%20class=%22&p=1
```

Doing so results in various links within the page to be modified, including the link tag:

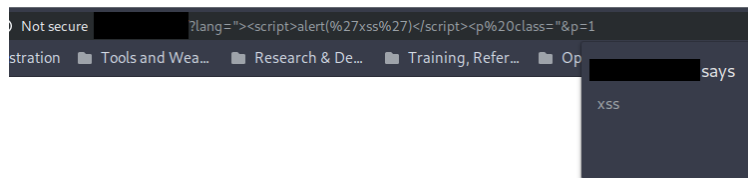[gist id="707aa537a707c558700b44ce3b6072d3" file="injected.html"]

And thus results in execution of JavaScript code:

Cross-Site- Scripting of the CLink Office v2 Control Panel via the lang parameter

Conclusion

Most control panels nowadays are leveraging frameworks and libraries that are filtering inputs from clients, however, this specific case shows that custom-made scripts are still out there. These should be avoided by clients seeking hosting services and request hosting companies to employ validated and verified software. *CommuniLink* was first contacted on 7 Jan 2020 and a second time on 13 Jan 2020. HKCERT was contacted on 2 Mar 2020. No answer was received and a such this vulnerability is disclosed after 90 days of discovery.

Home(https://www.deepcode.ca/)　　About Us(https://www.deepcode.ca/index.php/about-us/)

Contact(https://www.deepcode.ca/index.php/contact-deepcode/)

(https://www.linkedin.com/company/deepcodesec/)

(https://github.com/DeepCodeSec)

(https://t.me/deepcodesec)

Privacy & Policy　　Terms and Conditions

⊕ Top