[AIT-SA-20210215-04] CVE-2020-24036: ForkCMS PHP Object Injection

From: sec-advisory <sec-advisory () ait ac at>
Date: Fri, 12 Mar 2021 10:50:01 +0000

~~~~
ForkCMS PHP Object Injection
=========================
| Identifier: | AIT-SA-20210215-04 |
| Target: | ForkCMS |
| Vendor: | ForkCMS |
| Version: | all versions below version 5.8.3 |
| CVE: | CVE-2020-24036 |
| Accessibility: | Remote |
| Severity: | Medium |
| Author: | Wolfgang Hotwagner (AIT Austrian Institute of Technology) |

SUMMARY
=========
[ForkCMS is an open source cms written in PHP.](https://www.fork-cms.com/)

VULNERABILITY DESCRIPTION
========================
PHP object injection in the Ajax-endpoint of the backend in ForkCMS below version 5.8.3 allows authenticated remote
user to execute malicious code.

The ajax-callbacks for the backend use unserialize without restrictions or any validations. An authenticated user
could
abuse this to inject malicious PHP-Objects which could lead to remote code execution:

```
<?php

namespace Backend\Core\Ajax;

use Backend\Core\Engine\Base\AjaxAction as BackendBaseAJAXAction;

use Symfony\Component\HttpFoundation\Response;

/**

 * This action will generate a valid url based upon the submitted url.

 */

class GenerateUrl extends BackendBaseAJAXAction

{

    public function execute(): void

    {

        // call parent, this will probably add some general CSS/JS or other required files

        parent::execute();

        // get parameters

        $url = $this->getRequest()->request->get('url', '');

        $className = $this->getRequest()->request->get('className', '');

        $methodName = $this->getRequest()->request->get('methodName', '');

        $parameters = $this->getRequest()->request->get('parameters', '');

        // cleanup values

        $parameters = unserialize($parameters); // ← VULNERABLE CODE

        // fetch generated meta url

        $url = urldecode($this->get('fork.repository.meta')->generateUrl($url, $className, $methodName, $parameters));

        // output

        $this->output(Response::HTTP_OK, $url);

    }

}
```

PROOF OF CONCEPT
=================
In order to exploit this vulnerability, an attacker has to be authenticated with least privileges. We tested this
exploit with “Dashboard” permissions.

For demonstration purposes we created a proof of concept exploit that deletes files and directories from the
webserver.
With more effort an attacker might also find a payload for executing a webshell. There are many gadgets available in
the vendor directory for potential payloads.

The object-injection code for generating a payload might look as following:

```
'O:27:"Swift_KeyCache_DiskKeyCache":1:{s:4:"keys";a:1:{s:%d:"%s";a:1:{s:%d:"%s";s:9:"something";}}}' %
(len(filepath),filepath,len(deletefile),deletefile)
```

VULNERABLE VERSIONS
===================
All versions including 5.8.1 are affected.

TESTED VERSIONS
===============
ForkCMS 5.8.1 (with Debian 10 and PHP 7.3.14-1)

IMPACT
======
An authenticated user with minimal privileges could execute malicious code.


MITIGATION
==========
Fork-5.8.3 fixed that issue

VENDOR CONTACT TIMELINE
~~~~

```
========================
| 2020-05-01 | Contacting the vendor |
| 2020-06-08 | Vendor replied |
| 2020-07-07 | Vendor released an updated version |
| 2021-02-15  | Public disclosure |

ADVISORY URL
============
[https://www.ait.ac.at/ait-sa-20210215-04-poi-forkcms](https://www.ait.ac.at/ait-sa-20210215-04-poi-forkcms)
```

By Date   By Thread

Current thread:

[AIT-SA-20210215-04] CVE-2020-24036: ForkCMS PHP Object Injection *sec-advisory (Mar 12)*

Site Search

Nmap Security Scanner
- Ref Guide
- Install Guide
- Docs
- Download
- Nmap OEM

Npcap packet capture
- User's Guide
- API docs
- Download
- Npcap OEM

Security Lists
- Nmap Announce
- Nmap Dev
- Full Disclosure
- Open Source Security
- BreachExchange

Security Tools
- Vuln scanners
- Password audit
- Web scanners
- Wireless
- Exploitation

About
- About/Contact
- Privacy
- Advertising
- Nmap Public Source License