dahua966 Create XXE_modxcms.md History

1 contributor

22 lines (17 sloc) | 761 Bytes

XXE in ModxCMS

The link for CMS: https://github.com/modxcms/revolution.

There is a very serious XXE vulnerability in core\model\modx\rest\modrestservice.class.php, which could lead to sensitive information leakage or DoS attack. In function _collectRequestParameters, the user input is parsed directly without any sanitation. When the content type is text/xml, it will lead to XXE attack.

```
        protected function _collectRequestParameters() {
        $filehandle = fopen('php://input', "r");
....
        switch ($contentType) {
....
            case 'text/xml':
                $data = stream_get_contents($filehandle);
                fclose($filehandle);
                $xml = simplexml_load_string($data);
```

This vulnerability has been fixed.