# **TEMPLATE-VULN-NAME**

## DATE – *5/20/2016*

## EXPLOIT TYPE – *File Upload*

## DELIVERY METHOD – *GET Request* (via webpage, file, network protocol, LPE, other)

|  |  |
| --- | --- |
| AFFECTED SYSTEMS AND USE CASE | |
| Affected Platforms | All |
| Affected Platforms Versions | All |
| Number of Affected Users (est) | Unknown |
| Demographic /  Use of Affected Platform | Enterprise Backup Solution |
| Vulnerable Application | Unitrends |
| Vulnerable Application Versions | 8.X and below. |
| Affect Current Version? (Y/N) | Y |
| Use Case / Value Proposition | Given a valid user account, a user can upload a web shell onto the server to execute arbitrary code. |

|  |  |
| --- | --- |
| EXPLOIT DETAILS |  |
| Bug Class | File Upload |
| Number of Bugs | 1 |
| Exploit Reliability | 100% |
| How many seconds does exploitation take? Specific Configurations take longer? | Depends on server processing time for HTTP requests. |
| Privilege Level Gained | Apache (Or whatever user is running the web application) |
| Minimum Privilege Required for Exploitation | Valid user credentials. |

|  |  |
| --- | --- |
| MITIGATION AND ALERTS | |
| Exploitation Parameters  (Affected by / provides bypass for DEP / ASLR / Sandboxing / etc) | Several. Many parameters work in tandem to create the webpage. |
| Alerts target user? | No. |
| Require writing to disk? | Yes. |
| Require specific target user interaction? | No. |

|  |  |
| --- | --- |
| ADVANCED DETAILS | |
| Compatible with arbitrary payloads? | No, there is a limit to the length of an HTTP GET request. |
| Any caveats or environmental factors?  (payload size restrictions, encoding issues, JavaScript Requirements, etc) | You must write to a directory where the webserver user can write. |
| List deliverables including documentation. | Vulnerable code walkthrough and example request. |
| Provide detailed testing instructions. | 1. Login to the application. 2. Send the payload to the vulnerable endpoint. |
| Provide complete description of the vulnerability and exploit process. | The user needs to login to the application. From there, the user should issue the request to the vulnerable endpoint including the payload they wish to write to disk. To exploit, writing should be sent to the web-viewable and writable /var/www/html/tempPDF/ path. |

|  |  |
| --- | --- |
| TIMELINE / PRICING |  |
| Ready for delivery immediately? | Yes. |
| Non-Exclusive Pricing |  |
| Exclusive Pricing |  |