# **TEMPLATE-VULN-NAME**

## DATE – *5/20/2016*

## EXPLOIT TYPE - *sdfsdf*

## DELIVERY METHOD – *sdfsdf* (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 account, an attacker could execute arbitrary code on the machine. |

|  |  |
| --- | --- |
| EXPLOIT DETAILS |  |
| Bug Class | Remote Code Execution |
| Number of Bugs | 1 |
| Exploit Reliability | 100% |
| How many seconds does exploitation take? Specific Configurations take longer? | Depends on the speed a webserver can process a request. |
| Privilege Level Gained | The user who started the webserver process. |
| Minimum Privilege Required for Exploitation | Any valid user. |

|  |  |
| --- | --- |
| MITIGATION AND ALERTS | |
| Exploitation Parameters  (Affected by / provides bypass for DEP / ASLR / Sandboxing / etc) | Username |
| Alerts target user? | No, but the request will be logged in /tmp/cmc\_\*.log |
| Require writing to disk? | No |
| Require specific target user interaction? | No |

|  |  |
| --- | --- |
| ADVANCED DETAILS | |
| Compatible with arbitrary payloads? | Yes. |
| Any caveats or environmental factors?  (payload size restrictions, encoding issues, JavaScript Requirements, etc) | Depends on the architecture the affected webserver is running. |
| List deliverables including documentation. | Vulnerable code walkthrough along with an example request. |
| Provide detailed testing instructions. | Download the latest version of the Unitrends server and create an account. Navigate to the specified URL and send the payload. |
| Provide complete description of the vulnerability and exploit process. | Given a valid user account a user can execute arbitrary code. The process is:   1. Login to the application. 2. Send the payload. |

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