# **TEMPLATE-VULN-NAME**

## DATE – *5/20/2016*

## EXPLOIT TYPE – *Web Application Privilege Escalation*

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

|  |  |
| --- | --- |
| AFFECTED SYSTEMS AND USE CASE | |
| Affected Platforms | n/a |
| Affected Platforms Versions | n/a |
| Number of Affected Users (est) | n/a |
| Demographic /  Use of Affected Platform | Enterprise Backup Server |
| Vulnerable Application | Unitrends |
| Vulnerable Application Versions | 8.X and below. |
| Affect Current Version? (Y/N) | Y |
| Use Case / Value Proposition | Given a low level account to access the Unitrends console, one can escalate to root. |

|  |  |
| --- | --- |
| EXPLOIT DETAILS |  |
| Bug Class | LPE |
| Number of Bugs | 1 |
| Exploit Reliability | 100% |
| How many seconds does exploitation take? Specific Configurations take longer? | The length of time it takes to process a request. |
| Privilege Level Gained | root |
| Minimum Privilege Required for Exploitation | Authenticated user. |

|  |  |
| --- | --- |
| MITIGATION AND ALERTS | |
| Exploitation Parameters  (Affected by / provides bypass for DEP / ASLR / Sandboxing / etc) | The cookie “token.” |
| Alerts target user? | Your log file is written to with the new userID logging in. |
| Require writing to disk? | No. |
| Require specific target user interaction? | No. |

|  |  |
| --- | --- |
| ADVANCED DETAILS | |
| Compatible with arbitrary payloads? | No. |
| Any caveats or environmental factors?  (payload size restrictions, encoding issues, JavaScript Requirements, etc) | If the root user has been removed, fuzzing the payload may be required. However this is “simple” fuzzing, as you must enumerate the user ID. |
| List deliverables including documentation. | Exploit code and explanation. |
| Provide detailed testing instructions. | 1. Log into your web application. 2. Change your “token” cookie to the value described in the exploit. 3. Refresh the page. |
| Provide complete description of the vulnerability and exploit process. | The “token” value is susceptible to modification, allowing a user to flip out of their current session and into an administrative session. This is because each token issued is not checked against the user. |

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