

[VulnWatch] iDefense Security Advisory 04.02.07: Hewlett-Packard Mercury Quality Center ActiveX Control ProgColor Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-04/msg00001.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Mon, 02 Apr 2007 14:36:52 -0400
-

Hewlett-Packard Mercury Quality Center ActiveX Control ProgColor Buffer
Overflow Vulnerability

iDefense Security Advisory 04.02.07
<http://labs.iddefense.com/intelligence/vulnerabilities/>
Apr 02, 2007

I. BACKGROUND

Hewlett-Packard Mercury Quality Center is a web-based interface that allows managers to automate software quality testing. More information is available at URL shown below.

<http://www.mercury.com/us/products/quality-center/>

II. DESCRIPTION

Remote exploitation of a buffer overflow vulnerability in an ActiveX control installed by Hewlett-Packard Mercury Quality Center could allow for the execution of arbitrary code.

Hewlett-Packard Mercury Quality Center installs the following ActiveX control which is registered as safe for scripting.

ProgId: SPIDERLib.Loader
Clsid: 98C53984-8BF8-4D11-9B1C-C324FCA9CADE
File: C:\WINDOWS\Downloaded Program Files\Spider90.ocx

This control contains an exploitable stack based buffer overflow in the "ProgColor" property. By setting this property to an overly long value, a buffer overflow will occur.

III. ANALYSIS

Exploitation of this vulnerability allows for the execution of arbitrary code.

The target ActiveX Control is part of the Mercury Quality Center web application which runs on port 8080 by default. Any user which can remotely log into the web application will have to install the vulnerable control.

IV. DETECTION

iDefense has confirmed this vulnerability in the control that is installed with the 9.0 version of Hewlett–Packard Mercury Quality Center. The vulnerable ActiveX control is version 9.1.0.4353.

V. WORKAROUND

Setting the kill–bit for this control will prevent it from being loaded within Internet Explorer. However, doing so will prevent legitimate use of the control.

VI. VENDOR RESPONSE

Hewlett–Packard Mercury has addressed this vulnerability by releasing patches. For more information consult HP Document ID c00901872 via the URL shown below.

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00901872>

VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

VIII. DISCLOSURE TIMELINE

02/16/2007 Initial vendor notification
02/16/2007 Initial vendor response
04/02/2007 Forced public disclosure

IX. CREDIT

This vulnerability was reported to iDefense by Eric Detoisien, and Titon & Ri0t of Bastard Labs.

Get paid for vulnerability research
<http://labs.idefense.com/methodology/vulnerability/vcp.php>

Free tools, research and upcoming events
<http://labs.idefense.com/>

X. LEGAL NOTICES

Copyright © 2007 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please e-mail customerservice@xxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.