Is Your Online Help A Security Risk ?

A WebWorks.com White Paper.

Author:
Alan J. Porter
WebWorks.com
a brand of Quadralay Corporation
aporter@webworks.com

WW_WP0610_security

NOTE: Please feel free to redistribute this white paper to anyone you feel may benefit. If you would like an electronic copy for distribution, just send an e-mail to info@webworks.com

Overview

This paper will discuss issues relating to the security in online helps systems, and steps you can take to protect against potential threats.

Background

"I never considered that my online help could be a potential attack vector!"

The above quote from a WebWorks ePublisher customer buried in the text of an email really caught our attention. In many ways it served as a wake up call and a rallying cry for us to take a closer look at not only the security of our own WebWorks Help cross platform delivery product, but at the security risks related to the delivery of online help in general.

We received the email when working with a customer who had discovered a potential cross-site scripting threat in our WebWorks Help 5 online help product. A cross-site scripting vulnerability means that malicious attackers may inject a client side script into a web page, bypassing browser security restrictions.

Working with our customer and an independent security firm, we moved quickly to investigate, build and test remediation steps for the WebWorks Help product. The result of that rapid response was the release of a WebWorks Security Advisory on December 15th, 2009. The advisory included a code fix and documented remediation steps. The changes were also incorporated into the 2009.3 and 2009.4 releases of the ePublisher platform. This ensures that any WebWorks help deliverables built with those, and subsequent, releases would not be subject to the vulnerability.

We could have left it at that, but during the course of our investigations we came to believe that this was an issue that should be discussed more openly. We needed to raise a general awareness of how and why you need to look at your Online Help systems as a potential security risk.

We weren't alone.

In 2007 the security firm Symantec documented that cross-site scripting accounted for approximately 80% of all security vulnerabilities[1]. The impacts ranged from being a petty nuisance to attacks carrying significant risk.

Other online help systems have also been subject to the same vulnerability over the last few years. Adobe issued a total of nine security advisories for either RoboHelp or RoboHelp server between 2007 and 2009[2].

[1] Symantec Internet Security Threat Report, - http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf
[2] See http://www.adobe.com/support/security

Adobe, like WebWorks, has posted full details of these advisories on their websites, but we found during our investigations that other companies with tools in the editing / content management / publishing pipeline had issued advisories to their customers, but not necessarily posted the information online.

More to come.

While many companies have been working to combat this sort of vulnerability , hackers and malicious code writers move on to other targets. One of the most common alternatives to publishing Online Help in a browser is to produce traditional page based manual online using PDF.

However PDF may be just as prone to malicious attacks. According to leading security vendor McAfee's 2010 Threat Predictions Report[3], we should pay special attention to PDF. The report surmises that in 2010, "Adobe software, especially Acrobat Reader and Flash will take the top spot" among targets for hackers.

Already in 2010 (February) Adobe has issued a security update for the Acrobat reader[4].

It's not just the delivery platform either.

In 2009, over 110 security weak spots were reported in common browsers, Web applications, and operating systems. In January 2010, Microsoft issued two separate advisories for vulnerabilities related to every version of its Internet Explorer browser within two weeks of each other.

Why is Online Help particularly vulnerable?

Aside from potential vulnerabilities in delivery platforms and browsers, Online Help itself can often be more vulnerable than other web based applications for a variety of reasons.

- Traditionally Online Help is delivered on a "publish and forget" model. The Help system is linked to one particular version of a product or a project. Once a project is complete, the focus tends to turn to the next product. Online Help systems often go unmaintained.

- Even if an Online Help system is no longer active, many legacy systems stay live. They only need to be deployed once with an inbuilt vulnerability for them to become a potential attack vector. The fact that help systems are often overlooked can make them attractive targets for malicious code.

- Online help systems stay static delivered with and keyed to older versions of browsers that become more vulnerable as time progresses.

- Online Help is often overlooked by IT security audits as it is not generally considered part of IT infrastructure as "it's just documentation."

[3] http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf
[4] http://www.adobe.com/support/security/bulletins/apsb10-07.html

Don't forget about internal threats.

While most companies focus the bulk of their IT security monitoring on external threats, internal attacks represent the greatest area of potential security threats. Internal phishing attacks are the best way to engineer data loss and are particularly prone to cross-site scripting attacks. Malicious employees may access logins to systems were they do not normally have access, such as HR and Payroll records. While a company may inherently trust its employees, those trusted employees have far greater power to affect corporate systems..

Trusted employees can also be compromised by external elements, particularly as more companies open up their internet restrictions to enable employee participation in social networks and online communities. This collaborative participation is an increasing part of doing business and staying competitive in the changing digital landscape.

Security is about process.

Good security is not just about patching holes, it's about developing a process to both fix the current issue and protect against potential future threats. While a single deliverable may be vulnerable, a well defined process should account for this and remedy it over time.

For document production we recommend that you develop a process to refresh on a schedule. For example Microsoft has the concept of a "Patch Tuesday," where on the second Tuesday of each month, it releases security patches. While you may not need to update your Online Help deliverables on such an aggressive schedule, the same philosophy of regular updates should also apply to documentation.

Taking steps to ensure that you are protected.

Over the course of our investigations we have developed the following recommendations to help reduce the possibility of your Online Help becoming a security risk.

- Keep online delivery platforms up to date. Whenever possible use the latest versions of the software available in your production line. Keep up to date on upgrades and patches.
- Use the latest version of browsers where ever possible.
- Watch for Security Advisories issued by your vendors. In fact, ask all your vendors if they have ever issued security advisories (remember that not all of them make advisories public).
- If your vendors do issue security advisories, review them, test to see if they apply and if they do ACT on them. Apply any recommended remediation steps, and upgrade to the next release.
- Develop a process to periodically refresh your Online Help deliverables using the latest versions of your production tools.

Summary

We should ALWAYS consider that online help could be a potential attack vector!

- Set up a systematic process to detect and protect.
- Keep tools and deliverables up to date.
- Remember not all security attacks come from the outside.
- Watch, listen and act.

webworks.com

About ePublisher

ePublisher enables cost-effective processes for efficiently writing, presenting, and deploying online and print publications. Through the use of its three components, organizations can leverage existing authoring tools and content management systems and meet organization-wide publishing needs without incurring expensive training or software deployment initiatives. Its open system architecture, based on industry-standard XSL, enables a large degree of flexibility, customizability, and migration investment protection.

ePublisher will save your group time and seamlessly fit into your writing workflow, giving your writers more time to do what they do best - write.

About WebWorks.com

WebWorks.com, a brand of Quadralay Corporation, is the leading provider of comprehensive online publishing and help system delivery solutions. Its products and services constitute the definitive single source for all your ePublishing needs. We specialize in content conversion software that outputs Web, online help, wiki, and electronic publication formats. Our ePublisher Platform can automate the conversion of source documents in popular authoring formats such as DITA-XML, FrameMaker or Word and convert them to multiple end-user formats such as wikis, mobile devices, WebWorks Help, HTML, CHM, and PDF. Our conversion system is based on XSL so that output formats can be customized or even developed from scratch..

Contact

Phone: 1-877-8-WEBWORKS
Email: info@webworks.com
Web: http://www.webworks.com