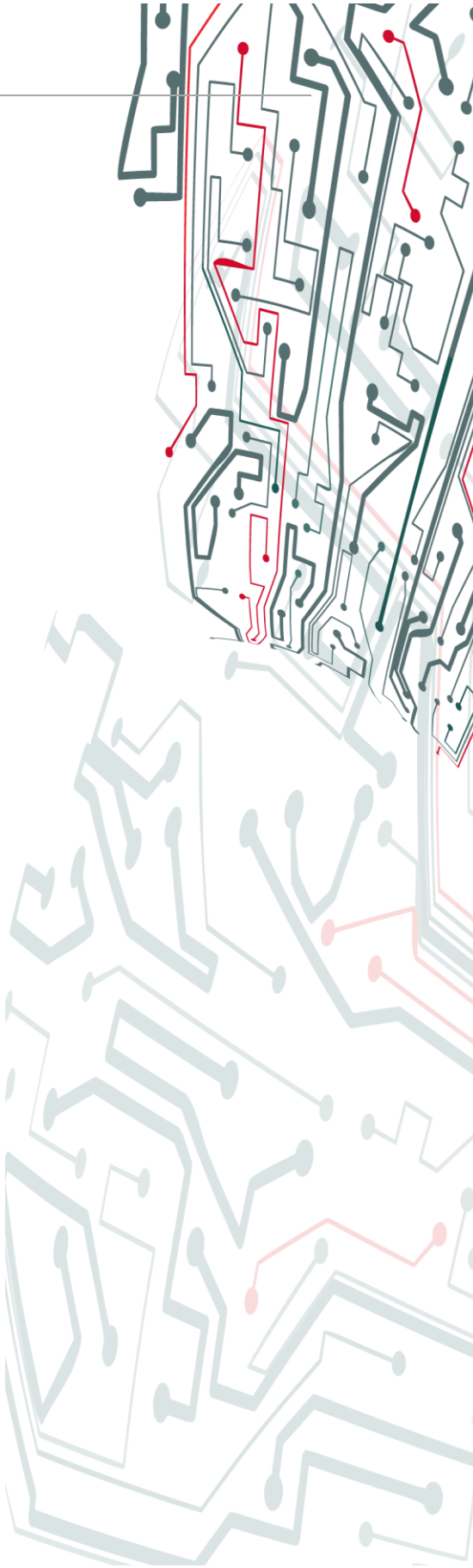
Adobe Reader 9

Security Best Practices



IOActive™

Comprehensive Information Security

Introduction

Adobe products have long touted how they enable organizations to collaborate and share information in heterogeneous environments. But a recent stream of vulnerabilities found in Adobe products has caused a great deal of concern about the overall security threat associated with using these products. The United States Computer Readiness Team's (US-CERT) advised against using Adobe Reader 9, recommending that, "users disable JavaScript in the application as a general workaround."

Stephen Northcutt, president of the SANS Institute warned, "I think organizations should avoid Adobe if possible. Adobe security appears to be out of control, and using their products seems to put your organization at risk. Try to minimize your attack surface. Limit the use of Adobe products whenever you can."

Understanding the importance that organizations place on these products, IOActive has done extensive research into Adobe Reader and prepared the following guidelines to how users can more securely leverage the benefits of Adobe Reader.

Background on IOActive's Research

Adobe Reader software is the global standard for electronic document sharing, and it is the only PDF file viewer that can open and interact with all PDF documents. Adobe Reader allows users to view, search, digitally sign, verify, print, and collaborate on Adobe PDF files.

Several JavaScript methods of the Document Object do not honor the Privileged Context and Safe Path settings. Independent research performed by Richard van Eeden, Senior Security Consultant at IOActive, uncovered a vulnerability that enabled execution of certain privileged JavaScript methods because Reader contains a vulnerability that supports calling "secure" functions in a non-secure context. This capability can be used to create or write to any files or folders on a targeted file system to which the attacker has access, resulting in:

- Possible full-system compromise simply by opening the malicious PDF—this could be propagated by way of email and written using a combination of privilege escalation, arbitrary file writing, and writing to PDF.
- System configuration files being written to, reconfiguring and opening the system up to further attack with insecure settings.
- User files being and network shares being written to, altering or deleting their content.
- A startup script being written to, forcing the system to perform arbitrary commands; this includes privilege escalation to the root/administrator level.

IOActive assigned this vulnerability a Severity Rating of High. Read the full security bulletin here. The Adobe Reader 9.2 update can be obtained here.

Best Practices

IOActive provides these recommendations based on security considerations that one should always keep in mind.

1. Update to the most recent version of Adobe Reader and install all relevant security patches.

   Security patches are the first line of defense against discovered vulnerabilities and known flaws, and should be installed regularly. Consider subscribing to release bulletins so that you can stay abreast of the most current information.

2. Disable JavaScript.

   Since the vulnerability is caused by Reader's use of JavaScript methods, disabling the scripting language is your best option until a remediation plan is created. This also is the current US-CERT recommendation.

3. Never open a document unless you know from where it came.

   This vulnerability can result in full-system compromise simply by opening a malicious PDF that was received by way of email.

4. Never visit an untrusted link.

   PDFs can be opened by way of the HTML iframe tag, which represents an inline frame that contains one HTML document inside a second HTML document. Visiting an untrusted link can result in an iframe opening a malicious PDF automatically. More information about the iframe tag.

5. If you must run Reader, do so with restricted privileges.

   Following the rule of least privilege is a standard security edict, meaning that users should operate their computer with the minimum set of privileges they need to do their job, typically operating as a standard user as opposed to an administrator. This is a problem because anything that runs or installs on an administrator's computer is done so with higher privileges. Restricting Reader's user privileges will place a tighter bound on what actions or exploits can occur.

6. Enable exploitation mitigation features such as ASLR and DEP.

   Since so many exploits rely on knowing where specific processes or system functions reside in memory, IOActive recommends employing mitigation features such as Address Space Layout Randomization—which arranges key data areas randomly in a

process' address space—and Data Execution Prevention—which prevents code execution from non-executable memory regions. More information about Data Execution Prevention. More information about Address Space Layout Randomization.