



# **Guidance on Handling Files with Possible Malicious Content**

GovCertUK Technical Note

Issued 13/02/2007

## **Key Points**

- The concept of a “safe” file format no longer exists.
- Education of users plays a key role in security.
- Only enable the minimal package functionality required.
- Content checkers and virus scanners can help reduce the risks.

## **Executive Summary**

The style of attacks being seen on the Internet has recently had a change of focus, leading us to conclude that existing advice on identifying potentially dangerous files is no longer valid.

Data types and file formats are now intended for distribution and sharing between the largest set of operating systems and software packages yet seen, opening up new freedoms in exploitation possibilities. Evidence suggests that the hacking community is increasingly interested in data files and common Internet Applications (such as Adobe Acrobat) and that they are using these for malicious purposes.

There are two main categories of attack. In one case, apparently ordinary documents are received, but subtle formatting within the document 'confuses' the application into allowing code execution. In the second, increased functionality within applications renders security models invalid and simply allows the attacker to do more than was previously possible.

Defence against these attacks will initially be difficult to conduct, since many new features and their associated software will need to be understood. Initial advice is to concentrate on maintaining a programme of user education that includes these new threats and implementing a series of technical measures, such as those detailed at the end of this document.

## **Introduction**

1. The objective of this Technical Note is to provide guidance to the GovCertUK constituency on the increasing use of traditionally passive data file types by the hacker community for delivering malicious executable code. The intended audience of this note is system administrators and organisational security officers who need to assess the risk of accepting files into the organisational security domain.

2. A change in the attack vectors currently in use by the hacking community, which is likely to continue in the short term, means that a change in advice is required to preserve the current level of security provided to public sector networks. Previous advice on this subject rated the risk of compromise depending upon the file type the user had received and/or opened. This approach to the subject is no longer valid and is in fact likely to reduce the effectiveness of the security barriers put in place. Therefore a new approach will be presented in this document.

3. The many options available, both to security personnel and attackers, means that there is no single solution. We will instead provide guidance on the type of threats likely to be encountered and best practice mitigation advice (which is presented at the end of this document).

## **Current Environment**

4. As indicated, previous guidance has focused on the type of file being accessed by the user. Happily, increased user awareness, security warnings issued by user applications and deployment of anti-virus technologies have all combined to mitigate much of this risk. Now, due to the incremental evolution of common applications (such as Adobe Acrobat) and increased interest in data files by the hacker community in general, the risk now comes from what was traditionally thought of as passive data formats. These include image files (".JPG", ".GIF" and ".PNG") and more complex, but common, document formats such as Microsoft Office (".DOC", ".XLS" and ".PPT") and Portable Document Format (".PDF") many of which will automatically render in browsers or e-mail applications and are routinely exchanged by users (with or without virus checking).

5. Unfortunately patching and the use of current best-practice technologies (such as anti-virus products and boundary content filtering devices) provide only retrospective protection against these threats. (How do you detect a legitimate feature being used maliciously or a logic error in a complex application?)

6. As the file formats have become more complex the need for more sophisticated and secure parser and rendering software has increased. As ever when new software is released, bugs and weaknesses in security models provide the attacker with new opportunities.

7. A new epoch in file format complexity is about to open. Data and file formats will be intended for distribution and sharing between the largest set of operating systems and software packages yet seen. This new freedom of working will also open up new freedoms in exploitation possibilities.

8. These new opportunities can be grouped into two main categories:

- Malformed data, rendered by user applications, causing code execution due to buffer-overflows or other logical errors.
- Ever more feature-rich applications, requiring complex data file formats, supporting features that could potentially be exploited maliciously “by design”.

9. The active exploitation of these new complex and feature rich file formats represents a current and growing threat. Attacks are seen every day involving the delivery of deliberately malformed content aimed at the unwary or uneducated user.

10. The following table demonstrates the variety and regularity of attacks seen during the last 18 months.

Year	Month	File Type
2007	January	ICS
2006	December	WMP, XLS
	November	SWF
	October	PPT, XLS, DOC
	September	PUB
	August	PPT
	July	XLS
	June	WMF, EMF, PNG, ART, MHT
	May	SWF
	April	WAB
	February	BMP
2005	January	EOT
	October	AVI, LNK
	August	JPG

**Fig 1. Example of Variety & Regularity of Attacks**

## Recommendations

11. The following advice should be passed on to each user community, together with an explanation concerning the latest threat potential:

- a) Do not open any unusual or suspicious e-mails or attachments. If you reply to a mail asking about its contents use a previously known address, this will not always be the one on the mail.
- b) Take notice of web browser security bar warnings (these are becoming more commonplace and users should be trained to adhere to content blocking policies – do you really need to view the blocked content? Do you know what you're about to allow?).
- c) Always treat attachments (or any imported data) as un-trusted and potentially malicious regardless of who appears to have sent it. Embedded images are potentially just as dangerous as application attachments.
- d) If unexpected data is received always try to verify the data with the originator before opening (if this is via e-mail try to use a previously known address, not the one on the unexpected mail). If possible use digital signatures when sending data.

12. System administrators are advised to carry out all of the following:

- a) Invest (or reinvest) in user awareness training.
- b) Make full use of any Operating System lockdown procedures available (see Government or vendor information).
- c) Consider limiting the functionality of common applications (by configuration changes) to the sub-set required to support the business – do you really use all the features, if not then why have them enabled?
- d) Try and adopt a "Save, Verify and then View" policy for un-trusted data files on the network. This might mean changing browser or e-mail configurations to not automatically view common file types instead prompting to save them to disk before opening.
- e) In the case of files sent as email attachments, some mail servers and mail clients (Microsoft Exchange and Outlook for example) can also be configured to block mail attachments with a given extension. It is recommended that this functionality be used.
- f) Ensure that the latest security patches are installed for all software. If possible verify that patches do not adversely affect system stability by testing in a non-operational environment.
- g) Install anti-virus products on workstations, servers and gateways. You should consider using an anti-virus product from a different vendor at each of these points to maximise the chances of detecting a virus.
- h) Check the configuration of anti-virus products for "heuristics" or "unknown virus" options. If these are not enabled, then enable them. Heuristic scanners look for suspicious code, and thus are an extra layer of defence when dealing with new viruses that are not specifically known to the anti-

virus product. This increases the chances of a new or sophisticated virus being detected. (There is a risk of the heuristic scanner incorrectly detecting a file as a virus. A review of the file in a quarantined environment may indicate that it is safe to provide to the recipient.)

- i) Update anti-virus products on a regular basis, preferably using automated update functionality to the organisational gateway.
- j) Use a content scanner at the gateway to check that the format of a file is as claimed, in conjunction with other personal/corporate protection products (anti-virus/firewall). Content checkers should be evaluated as fit for use before deployment (for example, against Common Criteria or the UK government's FASTRACK scheme), otherwise they may not provide the desired security functionality.