



Guidance Notes

Writing Advisories

**Andrew Cormack
JANET-CERT
UKERNA**

GD/NOTE/007

JANET Guidance Notes

JANET Guidance Notes are one of a series of user guides available to JANET customers. Guidance Notes do not generally contain detailed technical information and are primarily aimed at customers who wish to extend their general knowledge of a particular subject. These guides provide readers with a wide variety of general information, case studies and advice.

If you have any queries or comments about the Guidance Notes or would like to obtain copies, please contact:

JANET Customer Service

UKERNA

Atlas Centre, Chilton, Didcot

Oxfordshire, OX11 0QS

Tel: 0870 850 2212

Fax: 0870 850 2213

E-mail: service@janet.ac.uk

Further details of the documents in this series are available at:

<http://www.ja.net/documents/>

Contents

1	Introduction	5
2	Principles	5
3	Content	5
4	Sources	7
5	Credits and References	8
6	Finishing Touches	9
7	Further Information	9

1 Introduction

Advisory notices are a common means of disseminating information about new security threats or solutions. They are usually intended for use by groups of end users, whether workstation owners, system or network administrators, though managers may also read advisory notices to determine the level of risk and urgency of action. Advisories may be written by vendors, security teams or any other trusted parties in the networking world. Some teams issue different types of notice, with names such as warning, alert, notice, information, etc. In this document, the generic term advisory will be used, and should be taken to include all the various sub-advisories and local classifications.

Good advisories can be an effective way to improve the security of computers and networks, however badly written advisories can easily spread fear and confusion or destroy the trust that is essential to keep computer networks functioning.

This document is intended to be useful to the authors, or would-be authors, of advisories, to help them ensure that their efforts are of benefit of the network community. We hope it will also be useful to the recipients of advisories, to explain what authors should be trying to achieve and to help readers understand why demands that seem reasonable to them cannot always be met.

2 Principles

Computers can always be made more secure by better configuration or operating practice. However on some occasions new information may become available which makes a particular change more important. For example, a new vulnerability may be discovered that requires a patch to be installed to correct it, or changes in patterns of attack may increase the risk represented by a particular configuration or operating practice. In these circumstances it may be appropriate to distribute the new information in the form of an advisory notice.

The purpose of an advisory should always be to help improve the security of computers and networks. If an advisory will not result in an overall improvement then it must not be published. Obviously this means that every advisory must include at least one feasible remedy for the problem it describes. However a published advisory is, in effect, a public notice, so its effect on hostile users must also be considered. If the advisory will be of more use to them than to the well-intentioned computer user then it must not be published. In some cases even revealing that information is known by the security community may be of assistance to attackers.

If there is any doubt whether an advisory should be published then advice should be sought from experienced trusted parties in the security community, for example members of the Forum of Incident Response and Security Teams (FIRST), details of which can be found at:

<http://www.first.org/>

or the Computer Emergency Response Team (CERT) Co-ordination Center, details at:

<http://www.cert.org/>

All such communications, especially those that concern vulnerabilities that are not yet widely known, should be encrypted and signed to prevent accidental disclosure of information.

When dealing with newly discovered vulnerabilities that have not previously been published, authors should work with the vendors of the affected software or with another team experienced in vulnerability coordination. Such activities should always follow a published responsible disclosure process as set out, for example, in the National Infrastructure Advisory Council's Vulnerability Disclosure Framework (<http://www.dhs.gov/interweb/assetlibrary/vdwdgreport.pdf>).

3 Content

Advisories should always begin with a summary that enables readers to decide whether they are affected by the problem described, and whether to read further. If the advisory is to be sent by e-mail or published on the web then the subject or title will be part of this initial selection

process so these should be chosen with care. The summary section should be written to be accessible to all users, whether technical, management or end user. Later sections of the advisory may, where appropriate, be designed for a particular type of users. The summary will also be used by readers as part of their own risk assessment process. They may know of specific local circumstances that make a particular threat more or less serious in their own environment than in general.

The first paragraph should therefore always include the type of computer and operating system affected and any program or service that must be running to expose the problem. Software version numbers should be given where possible. If a range of version numbers is quoted, it should be made clear whether the given end points are affected or not, and authors should be aware that some products have version numbers where the sequence of releases may not be clear. The impact of the problem should be summarised - for example whether it is a potential denial of service, a local or root compromise - and an indication given of the urgency of dealing with the problem. Information may become available at different stages in the development of an attack: a problem may be theoretical, have been discussed in a public forum, have been demonstrated in a laboratory setting or have been seen 'in the wild'. The most urgent cases are usually those where an exploit tool is publicly available or where the problem is actively being used against the community for whom the advisory is written. A summary of the recommended remedial measures should be included in the summary with, if available, an indication of the expertise needed to implement the measure and the time that it is likely to take.

A checklist for preparing this introduction might be as follows:

- platform (system/OS and version);
- software (program/service and version);
- impact (information leak, Denial of Service (DoS), local privilege escalation, remote root compromise, etc.);
- threat (theoretical, demonstrated, wild, published exploit, active);
- type of remedy (patch, configuration change, router/firewall change, etc.);
- expertise and time required to implement remedy.

When using or referring to advisories or other material written by others, great care must be taken not to alter the meaning of the original text. This is particularly important when writing introductions or summaries, and when advisories are translated. Terms such as "may", "should", "some", "every" and "many" have been a common cause of problems as they are often understood differently by the author and the reader.

A unique reference should be included in the title or subject of the advisory as this will save confusion when others wish to refer to the advisory. If the advisory is likely to be distributed outside the constituency of the author team, then this reference should include a code that identifies that team. If advisories are updated with the same reference number, then each issue should be uniquely identified by its date (in UTC format) and version number; a revision history listing the versions and changes between each should also be included.

Following the introduction it may be helpful to include brief instructions of how to determine the version numbers of any operating systems or software mentioned in the text. These are not always easy to find from running programs.

Most of the rest of the advisory should consist of a description of measures that can be taken to address the problem. If there are multiple possible remedies, then these should be summarised first, making clear whether they should be regarded as permanent or short-term solutions and if any adverse effects can be expected. For example some services use Internet Protocol (IP) ports in the user range. Blocking access to these through a site router may prevent external attacks, but will also cause occasional failures of other services such as File Transfer Protocol (FTP).

Detailed instructions for installing patches or making major configuration changes are best referred to web sites, for example from vendors or Computer Security Incident Response Teams (CSIRTs). However, short examples such as how to comment a service out of `inetd.conf`, may usefully be included in the advisory itself. The advisory should include a reminder of any subsequent steps, such as stopping and restarting a service or rebooting the computer, that are needed to complete the remedy.

In some cases it may be helpful to include in the advisory some more detailed information about how the problem arises. However this should only be done where the information may help system administrators to determine whether their configuration is vulnerable, or to choose the most appropriate remedy. Great care should be taken to avoid publishing information that will give intruders significant help in exploiting a vulnerability.

For instance distributing sample exploit code, even if the example does not do damage, should be avoided as it is more likely to do harm than good. If users want to confirm empirically whether they are vulnerable this should be subject to individual discussion with their CSIRT and not the subject of a public announcement. Providing source code patches may itself be hazardous as this makes clear to intruders the exact nature of the problem. Remember that many system administrators will not take prompt action to address the problem. CSIRTs should not help intruders to attack these computers.

4 Sources

Information for advisories may come from a wide variety of sources, each of which has its own characteristics and uses. When using any information source it is important to consider: its reliability - how accurate is the information likely to be and how well-intentioned is the source; its timeliness - is the information available in time to protect systems against attack; detail, which needs to be both relevant to protecting systems, comprehensible and accurate.

For example:

- The fact that incidents are occurring definitely indicates that there is a problem but is unlikely to provide much detailed information as to how to resolve it. However if the service affected can be determined, perhaps from core files or log entries, then this information may be sufficient to make an advisory worthwhile. For example if a problem is known to relate to a particular, little used, service, then an advisory recommending that it be disabled, or its traffic blocked, may significantly reduce the number of exposed vulnerable systems even if no more information about the problem is available. In these circumstances it may be helpful to publish an advisory marked 'interim' to provide initial advice before a final version, based on more complete information, is issued.
- Information from 'full disclosure' mailing lists varies considerably in accuracy and intention, but is often available early in the life-cycle of a vulnerability. It may be extremely detailed, but the detail will often be more help in exploiting the problem than in resolving it. Such information should be used with caution (hoaxes and old news are quite common on these lists) and verified against other independent sources or local testing. It may well be worth delaying release of an advisory based solely on such material until its information can be confirmed by other means. Translating information from these mailing lists into a form that is helpful to the majority of users may involve significant effort.
- Some people make exploit tools available through mailing lists or web sites. This is usually current information, but even a detailed analysis of the tool will only indicate one specific way to exploit a vulnerability. Even if a fix can be reverse engineered from an attack tool, it may only protect against that particular implementation (virus signature files are the best known example of this approach). Attack tools alone are unlikely to identify the range of vulnerable systems and considerable effort is likely to be required to produce a beneficial advisory from only this information.
- An increasing number of vendors now publish information to help their customers protect themselves against vulnerabilities. This should be based on the best possible information - vendors have access to the source code after all - though there have been cases of security patches that introduced new problems of their own. Commercial pressure may lead vendors to take a different view from their customers of the risks of publishing an advisory: it is clearly tempting for them to play down the significance of a problem in their own systems. However there does seem to be an increasing and welcome move to openness by most commercial vendors.
- Independent commercial services can also be a source of high-quality information about vulnerabilities. The web sites of anti-virus vendors are a good example of this. Information from these sources is likely to be well focused on the user's need to remove the problem,

however the information may in some cases be restricted in how far it can be distributed. Such restrictions should always be obeyed, since they are the main way a provider can hope to make a profit. If information shared by these commercial sources is leaked then the sharing is likely to be withdrawn in future.

- Information in advisories from trusted CSIRTs should be reliable but is likely to become available later in the lifecycle of a vulnerability. However this information will usually be in a form that is immediately useful to users wishing to secure their own systems. Often all that is needed before passing on such information is to add an indication of the perceived local threat.

Whatever source of information is used, ensure that any conditions under which it was provided are respected. Some sources of information, for example FIRST mailing lists, are private unless the sender of information states otherwise. Such information must not be included in public advisories unless it is also available from other sources that are public. Other information sources may insist that the source of information be concealed or, conversely, that it be credited and certain conditions obeyed. Such conditions must always be respected otherwise information sources will simply be withdrawn.

5 Credits and References

Unless there is good reason not to do so, for example the explicit or implicit conditions mentioned above, advisories should give credit to the sources of information used in compiling them. For some sources the requirement to improve overall security may mean that a source should not be revealed, for example information that might identify a particular site or computer as suffering from a vulnerability should not normally be published; however if an organisation has spent its own time or effort in an investigation then it is fair to offer it the choice of credit or anonymity. There may also be good reason not to publicise details of web sites or mailing lists where exploits are discussed, compromises listed or tools distributed, if these are not already well known.

When referring to information or advisories published by others there may be a choice between including a copy in the advisory message and pointing to a version on the original web site. Provided the original is served from an easily accessible location with good connectivity it will usually be best to point to it. The slight disadvantage to readers of having to follow a hyperlink is probably outweighed by the likelihood that any changes to the information will be immediately visible and the courtesy to the provider of the information.

On the other hand, including the text of a third-party advisory within the author's allows recipients to verify PGP signatures on both parts of the advisory - web pages are rather hard to PGP sign as servers and browsers can modify the content in transmission. Including a particular version of the advisory text also permits detailed references to its content without the risk that these may cause confusion if the published version changes. Finally, if linking to the original is likely to result in the server or its connection being overloaded, then an alternative method should be chosen if possible. If in doubt, check what the preference of the originating site is. In any case, an advisory should always include the reference numbers of known advisories from other teams concerning the same vulnerability, as well as the vulnerability reference number assigned by the vendor and standard vulnerability databases such as Mitre's Common Vulnerabilities and Exposure project (<http://cve.mitre.org/>).

When distributing an advisory published by another team, these guidelines may result in an advisory that contains only a brief summary of the problem (sufficient for readers to decide whether it applies to them), an estimate of the local threat and a reference to a source. Busy readers will be very grateful for accurate, well-written advisories like this.

6 Finishing Touches

Although advisories are usually produced to a tight deadline, authors still owe it to their readers to ensure that they are professional documents. An advisory with faulty information may be worse than useless; an advisory that is hard to comprehend will simply be ignored. These problems can be avoided through a combination of human and computer assistance. Advisories should be spell-checked before publishing them; technical parts of the text are likely to throw up many 'errors' for filenames and commands, but the result will be much easier to read. If at all possible, advisories should be checked by another team member to ensure that they make sense and there are no obvious errors of fact. Debugging program code is much easier for someone other than the programmer, and errors in written documents are just as hard for the author to find.

When publishing an advisory be prepared to vouch for its authenticity and respond to any questions about it. All advisories should include contact details and should be digitally signed by the author or the organisation responsible for publication. Pretty Good Privacy (PGP) is the de facto standard for creating signatures, though X.509 certificates may become more accepted in time. Whatever form of signature is used, ensure that it can be easily checked: public keys should be placed in well-known repositories and certificates signed by international certification authorities. If the author has a web site or other obvious contact location, then make sure that readers can check his or her identity from there. Signatures are of no value unless readers verify them so it is the authors' duty to make this as easy as possible.

Finally, remember that having to retract an advisory or any statement in it is especially damaging for the reputation of a team. Before hitting the send or publish button, read the message through one more time to ensure it contains nothing you might come to regret.

7 Further Information

As the purpose of an advisory is to inform, the best judges of its quality are likely to be its recipients. When writing your own advisories, think of those you have received: which were helpful, and why, which were unhelpful and why. Look at examples from major players, for example vendors or major CERT teams, and try to learn both good and bad points from those. Kurt Seifried has done this for vendor advisories and published an article on the features he particularly likes and dislikes. This can be found at:

<http://www.seifried.org/security/articles/20010910-writing-security-advisories.html>

Other sources of, usually well-written, advisories include:

CERT-CC: <http://www.cert.org/advisories/>

CIAC: <http://www.ciac.org/ciac/>

Sun: <http://sunsolve.sun.com/pub-cgi/secBulletin.pl>

Cisco: <http://www.cisco.com/warp/public/707/advisory.html>

An excellent book on how to write programs with as few vulnerabilities as possible is

Graf, M & van Wyk, K, *Secure Coding: Principles and Practices*, O'Reilly [2003] ISBN 0-596-00242-4

The book has a website at <http://securecoding.org/>

Tell us what you think

Guidance Notes are produced and published by UKERNA for use within the JANET Community. We welcome your comments on all aspects of this document and on any other UKERNA publication. Please direct feedback to JANET Customer Service, at the address below, or e-mail us directly at:

documentation@ukerna.ac.uk

UKERNA manages the networking programme on behalf of the higher and further education and research community in the United Kingdom. JANET, the United Kingdom's academic and research network, is funded by the Joint Information Systems Committee (JISC).

For further information please contact:

JANET Customer Service
UKERNA
Atlas Centre, Chilton, Didcot
Oxfordshire, OX11 0QS

Tel: +44 (0) 1235 822 212
Fax: +44 (0) 1235 822 397
E-mail: service@janet.ac.uk

Copyright:

This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Availability:

Further copies of this document may be obtained from JANET Customer Service at the above address.

This document is also available electronically from: http://www.ja.net/documents/gn_advisories.pdf



© The JNT Association 2004

**Joint Information
Systems Committee**

