Vulnerability Handling Report Form

Vulnerability Handling is the process used to minimize the potential and consequences of compromise or abuse resulting from the necessary disclosure of information about security flaws in software systems. Vulnerabilities can be caused by software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems practices.

We encourage you to report any incidents you experience on your systems or any vulnerabilities you find. If you know of vulnerability in a product or if you have suspicious files please send us a sample for analysis (please zip the file), please complete below form and return it to vul_niser@niser.org.my. These reports will help us inform you and others about potential threats and ways to avoid or recover from them.

If we have additional questions, we will contact you for further information.
Thanks, we appreciate your taking the time to report this vulnerability.

CONTACT INFORMATION

Name : _____
E-mail : _____
Phone / fax : _____
Address : _____

Have you reported this to the vendor? [Yes/ No]_____

If so, please let us know whom you've contacted:

- Date of your report :_____
- Vendor contact name :_____
- Vendor contact phone :_____
- Vendor contact e-mail:_____
- Vendor reference number: _____

If not, we encourage you to do so vendors need to hear about vulnerabilities from you as a customer. We encourage communication between vendors and their customers. When we forward a report to the vendor, we include the reporter's name and contact information unless you let us know otherwise.

If you want this report to remain anonymous, please check here:

Do not release my identity to your vendor contact ☐

TECHNICAL INFO

If there is a MyCERT Special Alert /Advisory tracking number please put it here (otherwise leave blank): MA-# / MS-#_____.

a. Please describe the vulnerability.

_____

_____

_____

b. What is the impact of this vulnerability?

_____

(For example: can lead to denial service attack, create backdoor and steal password, etc.)

c) What is the specific impact?

_____

_____

_____

d) How would you envision it being used in an attack scenario?

_____

_____

e) To your knowledge is the vulnerability currently being exploited?
[Yes/ No]_____

f) If there is an exploitation script available, please include it here.

_____

_____

g) Do you know what systems and/or configurations are vulnerable?
[Yes/No]_____ (If yes, please list them below)

System :_____
OS version :_____
Verified/Guessed:_____

h) Are you aware of any workarounds and/or fixes for this vulnerability?
[Yes/No]_____
(If you have a workaround or are aware of patches please include the information here.)
_____
_____

OTHER INFORMATION

Is there anything else you would like to tell us?

_____

_____

_____