TWCERT/CC Common Vulnerabilities Exposure (CVE) example

TWCERT/CC
CVE Team

-Vulnerabilities Exposure Policy (in Chinese)：
http://surl.twcert.org.tw/gyRgA

==========

* Required field

-Report date*：
2019/04/11

-Contact information：
- Name*：Domo kun
- Organization：
- Email*：domokun@domo.tw
- Indicate here if you wish to remain anonymous*：☐ Yes ■ No

- Identification of Vulnerability*：
■ Self-observed
☐ Others：

- Date and Time of Identification*：2019/04/11
- Product Name*：badbutwork
- Product Version*：1.24
- Product Developer/Vendor*：techOh Inc.
- Product Website*：https://www.techoh.tw/

- Types of vulnerability*：Arbitrary code execution

- Vulnerability Description*：
Input parameter is not checked so this can be exploited for arbitrary code execution.

- Trigger Condition(s) of Vulnerability：

1. Any user can intrude the system and execute malicious scripts.

- Detailed Information of Trigger Method：

1. badbutwork -i cat /etc/passwd -t

- Additional Proof of Vulnerability：

Screenshot and recorded video as attachments.

- Impact of Vulnerability*：

An attacker can exploit this vulnerability using malicious script, and take over the system.

- CVSS v3 Score：

CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H

FIRST CVSS calculator：https://www.first.org/cvss/calculator/3.0

- Additional Information：

N/A