Radically Open Security

PENETRATION TESTING REPORT

for

ILLUMINATI INC

V0.1
Amsterdam,
November 4th, 2014

Document Properties

Client	Illuminati Inc
Title	Penetration Testing Report
Target	Illuminati NOC
Version	V0.1
Author	Alexander Author
Pen-testers	Fredik Nord; Fridolin Ord
Reviewd by	Richard Review
Approved by	Annabelle Approve
Classification	Confidential

Version Info

Version	Date	Author	Description
V0.1	November 4th, 2014	Alexander Author	Initial Draft

Contact

For more information about this Document and its contents please contact Radically Open Security BV.

Name	Constantin Contact
Address	Radically Open Security BV Overdiemerweg 28, 1111 PP Diemen
Phone	+00 11 22 33 44
Email	contact@example.com

Contents

1 Introduction **4**

1.1 Exploits 4

2 Findings **4**

3 Recommendations **5**

4 Conclusion **5**

1 Introduction

Here is the text of your introduction.

$$\alpha = \sqrt{\beta} \tag{1}$$

1.1 Exploits

```
Starting Nmap 6.47 ( http://nmap.org ) at 2014-8-7 20:32 CEST
Nmap scan report for audit001.test.net (82.199.82.183)
Host is up (0.034s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Nmap scan report for 88.111.88.111
Host is up (0.016s latency).
All 1000 scanned ports on 88.111.88.111 are filtered
Nmap scan report for audit002.test.net (88.111.88.111)
```

2 Findings

ID	Type	Description	Thread Level
AUD-001	Remote Code Execution	Unsanitized user input in the cgi script at allows logged-in users to execute arbitrary commands as the woops user on the blub host. The script generates and executes a commandline, which includes user input verbatim. By inserting, e.g., newline characters, the attack can break out of the intended commandline and execute arbitrary commands.	High
AUD-002	Remote Code Execution	Unsanitized user input in the cgi script at allows logged-in users to execute arbitrary commands as the woops user on the blub host. The script generates and executes a commandline, which includes user input verbatim. By inserting, e.g., newline characters, the attack can break out of the intended commandline and execute arbitrary commands.	High

3 Recommendations

ID	Type	Reccomendation
AUD-001	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-002	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-003	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-004	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.
AUD-005	Remote Code Execution	Update Fnord to the latest version, in which the vulnerable script has been removed.

4 Conclusion

Write your conclusion here.