S5L3

Report generated by Tenable Nessus™ Wed, 26 Feb 2025 09:50:26 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.40.101

1	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Feb 26 09:43:41 2025
End time: Wed Feb 26 09:50:26 2025

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.40.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

46882 - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277
https://seclists.org/fulldisclosure/2010/Jun/284
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	40820
CVE	CVE-2010-2075

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2010/06/14, Modified: 2022/04/11

Plugin Output

tcp/6667

```
The remote IRC server is running as :

uid=0(root) gid=0(root)
```