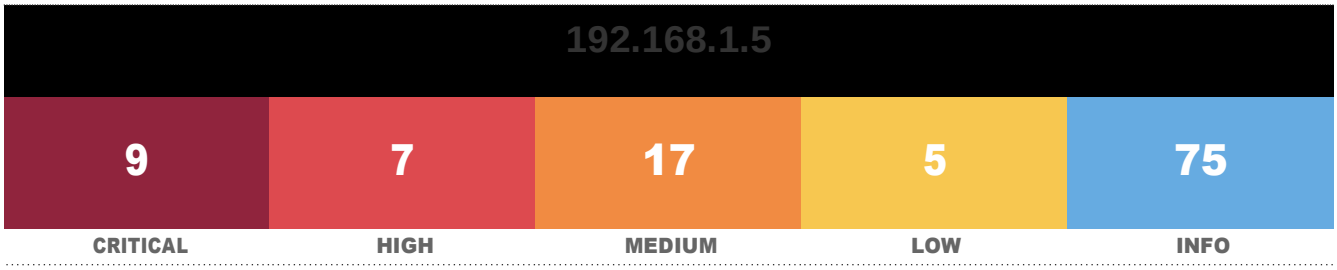
meta-Basic-scan

Report generated by Nessus™ Thu, 04 Aug 2022 08:25:56 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host



Vulnerabilities **Total: 113**

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	61708	VNC Server 'password' Password
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	136808	ISC BIND Denial of Service
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
HIGH	7.5*	10205	rlogin Service Detection
HIGH	7.5*	10245	rsh Service Detection
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

MEDIUM	6.5	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	57582	SSL Self-Signed Certificate
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	42263	Unencrypted Telnet Server
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6*	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	10407	X Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Il risultato del scansione di

Esempi di vulnerabilità

1- 46882 (1) - UnrealIRCd Backdoor Detection:

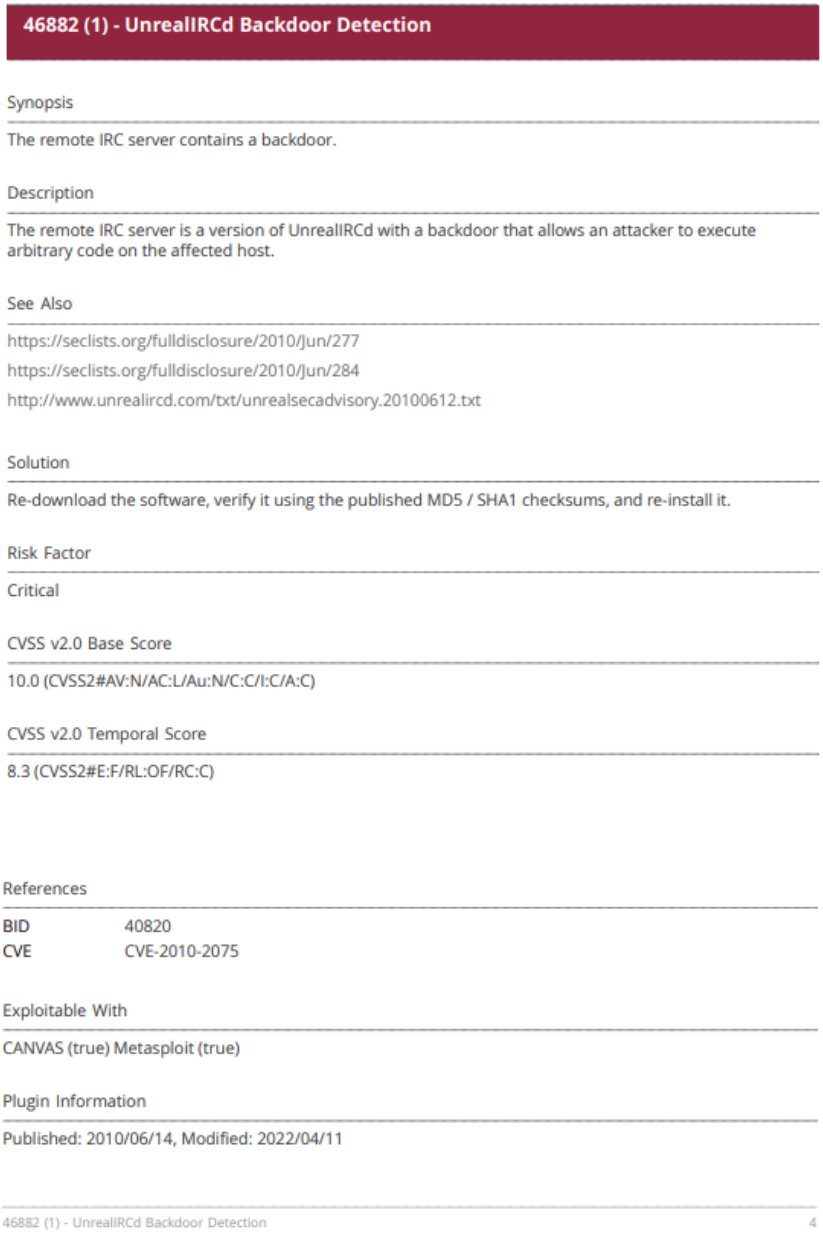
Indica che c'è una backdoor in (IRC) Internet Relay Chat

Descrizione:
Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente l'esecuzione a un utente malintenzionato codice arbitrario sull'host interessato.

Soluzione:
Scarica nuovamente il software, verificalo utilizzando i checksum MD5 / SHA1 pubblicati e reinstallalo.

Informazioni di risco
CVSS (Common vulnerability score system): è un framework aperto per comunicare le caratteristiche e la gravità delle vulnerabilità del software
CVSS v2: gravità delle vulnerabilità è 10
Significa molto grave (Criticale).

Dettagli CVE (Vulnerabilità ed esposizioni comuni**):** un elenco di falle di sicurezza del computer divulgate pubblicamente
CVE: CVE-2010-2075
BID: 40820



46882 (1) - 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

46882 (1) - UnrealIRCd Backdoor Detection 4

2- 136769 - ISC BIND Service Downgrade / Reflected DoS:

Indica che servizio ISC BIND è Downgrade
Che rifletta di un DoS (Denial of Service)

Scansione su porta 53 /UDP/DNS

Risk
Descrizione:
Secondo la sua versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita a sufficienza il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Soluzione:
Aggiornamento alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore
versione installato: 9.4.2
versione modificato: 9.11.19

Informazioni di risco
CVSS (Common vulnerability score system):
CVSS v3.0 Base Score 8.6
CVSS v3.0 Temporal Score 7.5
CVSS v2.0 Base Score 5.0
CVSS v2.0 Temporal Score 3.7
Significa e grave (Alta).

Dettagli CVE (Vulnerabilità ed esposizioni comuni)**:**
un elenco di falle di sicurezza del computer divulgate pubblicamente
CVE: CVE-2020-8616
XREF: IAVA:2020-A-0217-S

Vulnerabilities

136769 - ISC BIND Service Downgrade / Reflected DoS

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

See Also

https://kb.isc.org/docs/cve-2020-8616

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-8616
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2020/06/26

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```