延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-30	保存年限：2 年
日期： 115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-30-11506-01	版本：1.0

設備異動申請單

申請類別	□新增 □變更用途 □移撥 ■其它 弱點掃描修補		
資訊資產編號		資訊資產價值	
資訊資產名稱	書架系統、網域名稱系統		
申請說明：根據弱點掃描結果，修補 Ubuntu 已知弱點漏洞。			
申請人	黃韋霖	申請單位主管	延宇資訊股份有限公司 梁維志

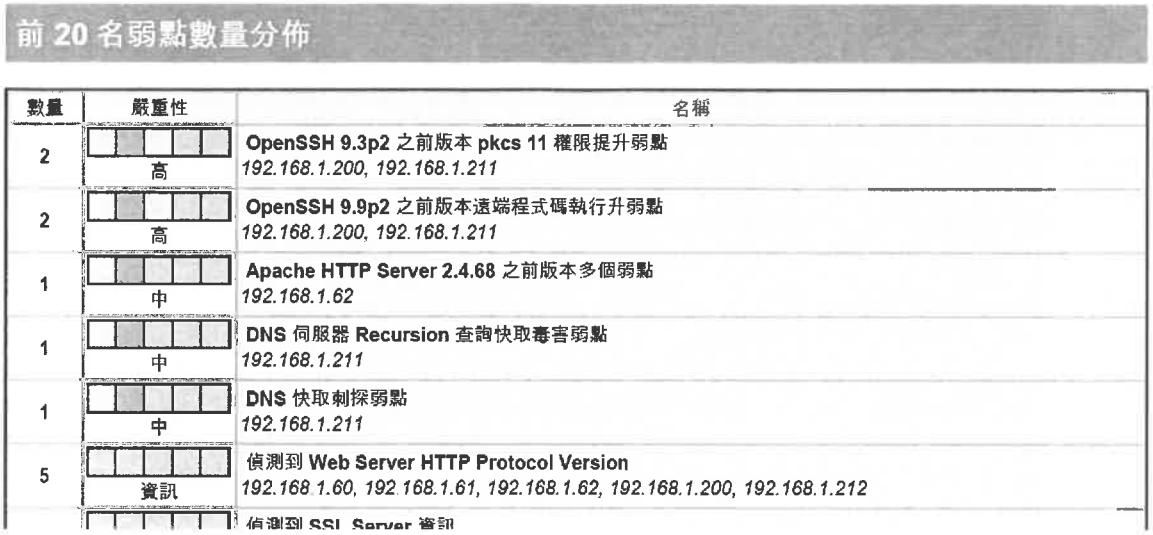
處理結果

☑同意 □不同意 說明：修補後已提供相關佐証。	若為設備變更用途或移撥，需查核下列事項： 1. 是否完成硬碟資料清除？ □是 ☑否 2. 是否移除授權軟體？ □是 ☑否
異動後資訊資產相關資訊如下：N/A 資訊資產編號：N/A 資訊資產名稱：N/A 資訊資產價值：N/A	

系統管理人員	資安長
黃韋霖	延宇資訊股份有限公司 梁維志

YAN-ISMS-G-30-11506-01 系統異動申請單-附件

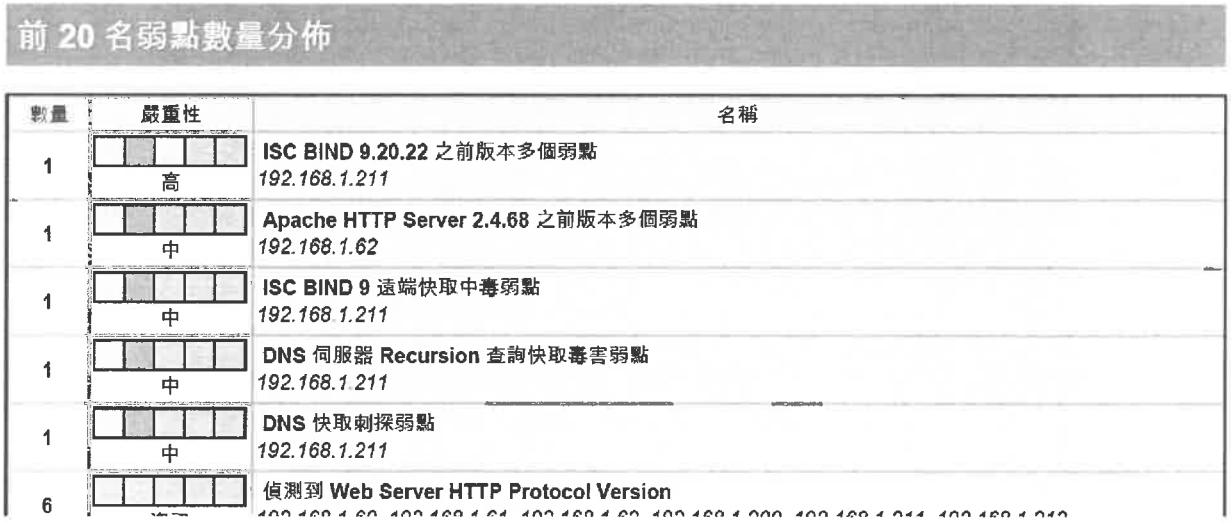
修補前：



前 20 名弱點數量分佈

數量	嚴重性	名稱
2	高	OpenSSH 9.3p2 之前版本 pkcs 11 權限提升弱點 192.168.1.200, 192.168.1.211
2	高	OpenSSH 9.9p2 之前版本遠端程式碼執行升弱點 192.168.1.200, 192.168.1.211
1	中	Apache HTTP Server 2.4.68 之前版本多個弱點 192.168.1.62
1	中	DNS 伺服器 Recursion 查詢快取毒害弱點 192.168.1.211
1	中	DNS 快取刺探弱點 192.168.1.211
5	資訊	偵測到 Web Server HTTP Protocol Version 192.168.1.60, 192.168.1.61, 192.168.1.62, 192.168.1.200, 192.168.1.212
		偵測到 SSL Server 資訊

修補後：



前 20 名弱點數量分佈

數量	嚴重性	名稱
1	高	ISC BIND 9.20.22 之前版本多個弱點 192.168.1.211
1	中	Apache HTTP Server 2.4.68 之前版本多個弱點 192.168.1.62
1	中	ISC BIND 9 遠端快取中毒弱點 192.168.1.211
1	中	DNS 伺服器 Recursion 查詢快取毒害弱點 192.168.1.211
1	中	DNS 快取刺探弱點 192.168.1.211
6		偵測到 Web Server HTTP Protocol Version

伺服器	弱點名稱	弱點項目
192.168.1.62	Apache HTTP Server 2.4.68 之前版本多個弱點	CVE-2026-49975
192.168.1.200	OpenSSH 9.3p2 之前版本 pkcs 11 權限提升弱點	CVE-2023-38408
	OpenSSH 9.9p2 之前版本遠端程式碼執行升弱點	CVE-2025-26465
192.168.1.211	ISC BIND 9.20.22 之前版本多個弱點	CVE-2026-3104
	ISC BIND 9 遠端快取中毒弱點	CVE-2007-2926
	DNS 伺服器 Recursion 查詢快取毒害弱點	CVE-1999-0024

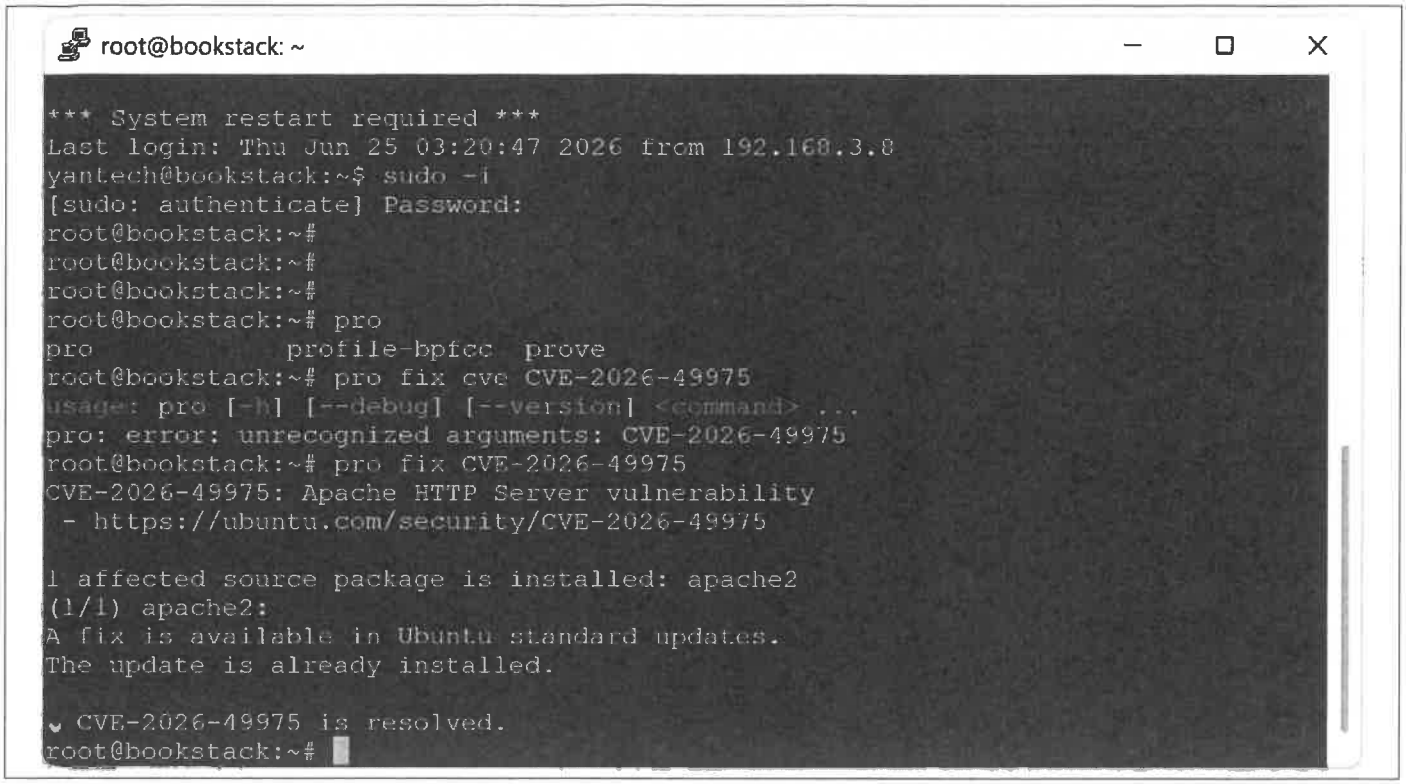
192.168.1.62(因 Ubuntu 穩定版號不會變更、但是已解決：Pro fix 佐證)



```
root@bookstack: ~
yantech@bookstack:~$ ^C
yantech@bookstack:~$ usermod -aG wheel yantech
usermod: group 'wheel' does not exist
yantech@bookstack:~$ sudo -i
root@bookstack:~#
root@bookstack:~#
root@bookstack:~#
root@bookstack:~# apt update && apt install --only-upgrade apache2
Hit:1 http://tw.archive.ubuntu.com/ubuntu resolute InRelease
Hit:2 http://tw.archive.ubuntu.com/ubuntu resolute-updates InRelease
Hit:3 http://tw.archive.ubuntu.com/ubuntu resolute-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu resolute-security InRelease
16 packages can be upgraded. Run 'apt list --upgradable' to see them.
apache2 is already the newest version (2.4.66-2ubuntu2.2).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 16
root@bookstack:~# apache2ctl -v
Server version: Apache/2.4.66 (Ubuntu)
Server built:   2026-06-03T15:25:00
root@bookstack:~# systemctl restart apache2
root@bookstack:~# apache2ctl -v
Server version: Apache/2.4.66 (Ubuntu)
Server built:   2026-06-03T15:25:00
root@bookstack:~#
```



```
root@bookstack: ~
yantech@bookstack:~$ sudo -i
root@bookstack:~#
root@bookstack:~#
root@bookstack:~#
root@bookstack:~# apt update && apt install --only-upgrade apache2
Hit:1 http://tw.archive.ubuntu.com/ubuntu resolute InRelease
Hit:2 http://tw.archive.ubuntu.com/ubuntu resolute-updates InRelease
Hit:3 http://tw.archive.ubuntu.com/ubuntu resolute-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu resolute-security InRelease
16 packages can be upgraded. Run 'apt list --upgradable' to see them.
apache2 is already the newest version (2.4.66-2ubuntu2.2).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 16
root@bookstack:~# apache2ctl -v
Server version: Apache/2.4.66 (Ubuntu)
Server built:   2026-06-03T15:25:00
root@bookstack:~# systemctl restart apache2
root@bookstack:~# apache2ctl -v
Server version: Apache/2.4.66 (Ubuntu)
Server built:   2026-06-03T15:25:00
root@bookstack:~# apt-get changelog apache2 | grep -i "2026-49975"
    - debian/patches/CVE-2026-49975.patch: fix cookie header accounting against
    - CVE-2026-49975
root@bookstack:~#
```



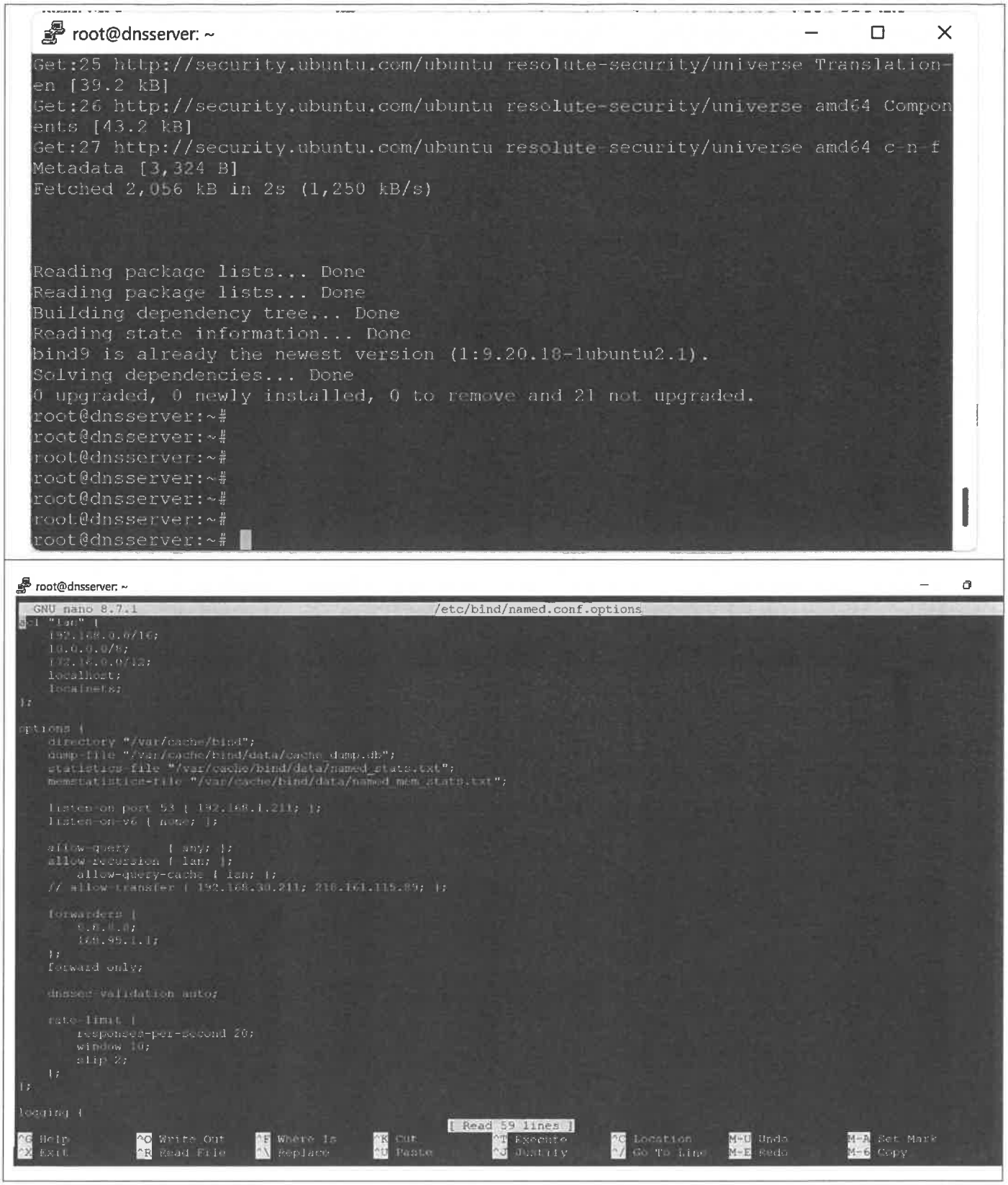
12

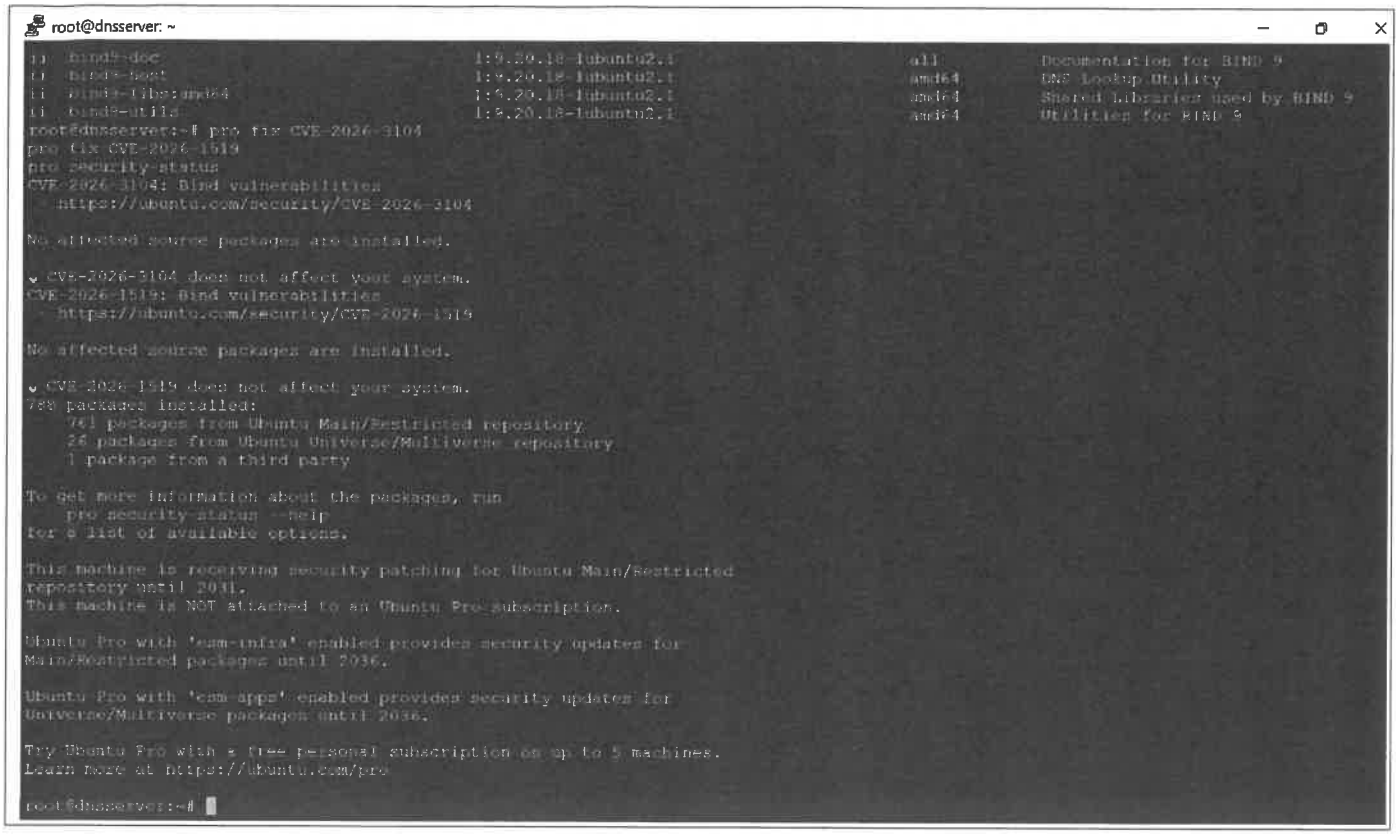
192.168.1.200(ESXI 已關閉 SSH)



192.168.1.200(DNS Server 已變更 OS 版本 CentOS8→Ubuntu 26.04，並修補漏洞)

19	WAN to DNS	all	DNS TCP DNS_UDP	always	DNS	接受	未啟用	全部	164.31 MB


root@dnsserver: ~
Get:25 http://security.ubuntu.com/ubuntu resolute-security/universe Translation-en [39.2 kB]
Get:26 http://security.ubuntu.com/ubuntu resolute-security/universe amd64 Components [43.2 kB]
Get:27 http://security.ubuntu.com/ubuntu resolute-security/universe amd64 c-n-f Metadata [3,324 B]
Fetched 2,056 kB in 2s (1,250 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bind9 is already the newest version (1:9.20.18-1ubuntu2.1).
Solving dependencies... Done
0 upgraded, 0 newly installed, 0 to remove and 21 not upgraded.
root@dnsserver:~#
root@dnsserver:~#
root@dnsserver:~#
root@dnsserver:~#
root@dnsserver:~#
root@dnsserver:~#
root@dnsserver:~#
root@dnsserver: ~
GNU nano 8.7.1
/etc/bind/named.conf.options
acl "lan" {
192.168.0.0/16;
10.0.0.0/8;
172.16.0.0/12;
localhost;
localnets;
};
options {
directory "/var/cache/bind";
dump-file "/var/cache/bind/data/cache_dump.db";
statistics-file "/var/cache/bind/data/named_stats.txt";
memstatistics-file "/var/cache/bind/data/named_mem_stats.txt";
listen-on port 53 { 192.168.1.211; };
listen-on-v6 { none; };
allow-query { any; };
allow-recursion { lan; };
allow-query-cache { lan; };
// allow-transfer { 192.168.30.211; 210.161.115.89; };
forwarders {
8.8.8.8;
168.95.1.1;
};
forward only;
dnssec-validation auto;
rate-limit {
responses-per-second 20;
window 10;
slip 2;
};
};
logging {
[Read 59 lines]
^G Help
^O Write Out
^F Where Is
^K Cut
^T Execute
^C Location
M-U Undo
M-A Set Mark
^X Exit
^R Read File
^\ Replace
^U Paste
^J Justify
^/ Go To Line
M-E Redo
M-6 Copy


root@dnsserver: ~
ii bind9-doc 1:9.20.18-1ubuntu2.1 all Documentation for BIND 9
ii bind9-host 1:9.20.18-1ubuntu2.1 amd64 DNS Lookup Utility
ii bind9-libs:amd64 1:9.20.18-1ubuntu2.1 amd64 Shared Libraries used by BIND 9
ii bind9-utils 1:9.20.18-1ubuntu2.1 amd64 Utilities for BIND 9
root@dnsserver:~# pro fix CVE-2026-3104
pro fix CVE-2026-1519
pro security-status
CVE-2026-3104: Bind vulnerabilities
https://ubuntu.com/security/CVE-2026-3104
No affected source packages are installed.
CVE-2026-3104 does not affect your system.
CVE-2026-1519: Bind vulnerabilities
https://ubuntu.com/security/CVE-2026-1519
No affected source packages are installed.
CVE-2026-1519 does not affect your system.
788 packages installed:
761 packages from Ubuntu Main/Restricted repository
26 packages from Ubuntu Universe/Multiverse repository
1 package from a third party
To get more information about the packages, run
pro security-status --help
for a list of available options.
This machine is receiving security patching for Ubuntu Main/Restricted
repository until 2031.
This machine is NOT attached to an Ubuntu Pro subscription.
Ubuntu Pro with 'esm-infra' enabled provides security updates for
Main/Restricted packages until 2036.
Ubuntu Pro with 'esm-apps' enabled provides security updates for
Universe/Multiverse packages until 2036.
Try Ubuntu Pro with a free personal subscription on up to 5 machines.
Learn more at https://ubuntu.com/pro
root@dnsserver:~#