受影響的節點：	其他資訊：
172.17.20.222:53	Vulnerable OS: Ubuntu Linux 18.04 Running DNS serviceProduct BIND exists -- ISC BIND 9.11.3Vulnerable version of product BIND found -- ISC BIND 9.11.3
172.17.20.223:53	Vulnerable OS: Ubuntu Linux 18.04 Running DNS serviceProduct BIND exists -- ISC BIND 9.11.3Vulnerable version of product BIND found -- ISC BIND 9.11.3
172.17.20.223:53	Vulnerable OS: Ubuntu Linux 18.04 Running DNS serviceProduct BIND exists -- ISC BIND 9.11.3Vulnerable version of product BIND found -- ISC BIND 9.11.3
172.17.20.224:53	Vulnerable OS: Ubuntu Linux 18.04 Running DNS serviceProduct BIND exists -- ISC BIND 9.11.3Vulnerable version of product BIND found -- ISC BIND 9.11.3
172.17.20.224:53	Vulnerable OS: Ubuntu Linux 18.04 Running DNS serviceProduct BIND exists -- ISC BIND 9.11.3Vulnerable version of product BIND found -- ISC BIND 9.11.3
172.17.20.225:53	Vulnerable OS: Ubuntu Linux 18.04 Running DNS serviceProduct BIND exists -- ISC BIND 9.11.3Vulnerable version of product BIND found -- ISC BIND 9.11.3
172.17.20.225:53	Vulnerable OS: Ubuntu Linux 18.04 Running DNS serviceProduct BIND exists -- ISC BIND 9.11.3Vulnerable version of product BIND found -- ISC BIND 9.11.3

參考：

來源	參考
CVE	CVE-2020-8625
DEBIAN	DSA-4857
URL	https://kb.isc.org/v1/docs/cve-2020-8625

漏洞解決方案：

更多關於升級 ISC BIND 的資訊請參考ISC 網站.

3.2.3. Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)

描述：

The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted. This could happen if: the chain/intermediate certificate is missing, expired or has been revoked; the server hostname does not match that configured in the certificate; the time/date is incorrect; or a self-signed certificate is being used. The use of a self-signed certificate is not recommended since it could indicate that a TLS/SSL man-in-the-middle attack is taking place

受影響的節點：