

Multiple DNS implementations vulnerable to cache poisoning

Summary

A vulnerability has been discovered in the DNS (Domain Name Service) protocol. This vulnerability affects any DNS server (all vendors are potentially affected), but also in a lesser way all DNS clients. This vulnerability could allow a remote attacker to corrupt DNS entries on vulnerable DNS servers and DNS clients. This corruption could allow a malicious person to redirect any network traffic (email, web, ftp, etc..) to a machine of his choice (DNS data of legitimate sites are corrupted).

Affected Products and Configurations

Currently only the VitalQIP product is directly impacted

Non-Affected Products and Configurations

Most of our deployed products are not affected.

Detailed vulnerability description

For details about this vulnerability and its impact we refer to <http://www.kb.cert.org/vuls/id/800113>

Solutions

Where required, new developments will take into account the mitigation actions. When one of our products is running on an affected platform, customers are urged to apply the corresponding platform patches in agreement with possible contractual arrangements

Specifically for the VitalQIP product, customers are advised to look for detailed information at <https://alerts.lucent.com/alerts/> (document 08-0555,08-0562, 08-0565).

References

Internal reference number: The vulnerability is tracked in the Alcatel-Lucent PSIRT database as VU-080709-1

Cert-IST reference number : Cert-IST/AV-2008.310

US-Cert reference : VU#800113

History

Date of document publishing on our external PSIRT website : august 5th, 2008

Vendor Statement

ALU is committed to continuously enhancing our security posture, and we have both internal and external resources involved in security review processes aimed at identifying product vulnerabilities, both in existing and in developing products.

It is important to note that there have been no reports of compromise due to this vulnerability. ALU's primary concern in this instance is to rapidly deploy a solution for our entire customer base. As a result, ALU has released patches for most code versions.



We highly recommend that you upgrade your products to a patch corresponding to your currently installed release. While we encourage customers to always utilize the latest releases to ensure the full benefit of our continued innovation and improvements, we recognize that this is not always possible. Information on our disclosure policy, how to report vulnerabilities and a list of public advisories can be found at our PSIRT website : <http://www1.alcatel-lucent.com/psirt>