Systems Affected

Misconfigured Domain Name System (DNS) servers that respond to global Asynchronous Transfer Full Range (AXFR) requests.

Overview

A remote unauthenticated user may request a DNS zone transfer from a public-facing DNS server. If improperly configured, the DNS server may respond with information about the requested zone, revealing internal network structure and potentially sensitive information.

Description

AXFR is a protocol for "zone transfers" for replication of DNS data across multiple DNS servers. Unlike normal DNS queries that require the user to know some DNS information ahead of time, AXFR queries reveal resource records including subdomain names [1](link is external). Because a zone transfer is a single query, it could be used by an adversary to efficiently obtain DNS data.

A well-known problem with DNS is that zone transfer requests can disclose domain information; for example, see CVE-1999-0532 and a 2002 CERT/CC white paper(link is external) [2][3](link is external). However, the issue has regained attention due to recent Internet scans still showing a large number of misconfigured DNS servers. Open-source, tested scripts are now available to scan for the possible exposure, increasing the likelihood of exploitation [4].

Impact

A remote unauthenticated user may observe internal network structure, learning information useful for other directed attacks.

Solution

Configure your DNS server to respond only to zone transfer (AXFR) requests from known IP addresses. Many open-source resources give instructions on reconfiguring your DNS server. For example, see this AXFR article for information on testing and fixing the configuration of a BIND DNS server. US-CERT does not endorse or support any particular product or vendor.

References

- [1] How the AXFR Protocol Works(link is external)
- [2] Vulnerability Summary for CVE-1999-0532
- [3] Securing an Internet Name Server(link is external)
- [4] Scanning Alexa's Top 1M for AXFR

Revisions

- April 13, 2015: Initial Release