The Infinitely Delegating Name Servers (iDNS) Attack

ANSSI – contact@cert.ssi.gouv.fr

The Domain Name System (DNS) is a hierarchical database, used to publish various content, ranging from IP addresses to administrative policies. One of its intrinsic property is also data decentralization. Indeed, domain name owners are allowed to delegate parts of their authority over a child domain (called a "sub-domain") to a third party. This third party is then able to store any content of his choice under this sub-domain or redelegate any sub-domains of it to yet another third party.

The ANSSI – the French Network and Information Security Agency – has uncovered a loophole in several implementations of DNS resolvers and the way they handle the DNS delegation mechanism. This loophole consists of an insufficient bounding (or the complete lack thereof) of the amount of work that a resolver is willing to do in order to resolve a domain name.

The Infinitely Delegating Name Servers Attack, described in the technical appendix, entices resolvers via a single query into following an infinite chain of delegations. Doing so may result in two types of denial of service situations. The exact nature of the denial of service varies from one implementation to an other.

On one hand, some implementations follow all the delegations at once, thus generating a network burst, leading to a distributed denial of service attack with high traffic amplification, in terms of packets. This burst uses legitimate and well-configured resolvers and does not require IP address spoofing to be triggered.

On the other hand, a sustained denial of service attempt, dwelling in the hundreds of thousands of "malicious" query/reponse exchanges between an attacker-controlled authoritative nameserver and the resolver under attack, can negatively affect the availability or the performance of the vulnerable DNS resolvers. The impact ranges from complete interruption of the service, to excessive resources consumption and to important reduction of the quality of service as well as noticable raise of the response time, on standard deployment scenarios.

All unpatched versions of BIND (CVE-2014-8500), Unbound (CVE-2014-8602) and PowerDNS Recursor (CVE-2014-8601) are vulnerable to this attack with various degrees of severity. The ANSSI also identified that BIND authoritative-only nameservers might also been vulnerable to the iDNS attack, when they host zones from untrusted parties. These software have been proven vulnerable in laboratory proof-of-concept experiments. The issue has also been confirmed by all DNS vendors, who provided a patch or a fixed version of their software. Patched versions are BIND 9.9.6-P1, BIND 9.10.1-P1, Unbound 1.5.1 and PowerDNS 3.6.2.

OpenDNS, Google Public DNS and Microsoft DNS on Windows Server 2012 implementations are not vulnerable.

The ANSSI recommends all DNS resolver software vendors to implement a bounding check on the amount of queries/work that can be generated in order to resolve a single domain name. OpenDNS, to whom the ANSSI asked for an operational feedback on these recommendations, confirmed they have already deployed similar mitigation strategies without impacting normal operations.

The ANSSI recommends network operators to upgrade their DNS software as soon as possible. The ANSSI also recommends network operators to evaluate the risk brought by the use of intermediate devices that could be overwhelmed by the network bursts generated by this attack or a variant thereof.