13.02.2024 – 17:09 Uhr

Serious Vulnerability in the Internet Infrastructure / Fundamental design flaw in DNSSEC discovered

Darmstadt and Frankfurt (ots) -

The National Research Center for Applied Cybersecurity ATHENE has uncovered a critical flaw in the design of DNSSEC, the Security Extensions of DNS (Domain Name System). DNS is one of the fundamental building blocks of the Internet. The design flaw has devastating consequences for essentially all DNSSEC-validating DNS implementations and public DNS providers, such as Google and Cloudflare. The ATHENE team, led by Prof. Dr. Haya Schulmann from Goethe University Frankfurt, developed "KeyTrap", a new class of attacks: with just a single DNS packet hackers could stall all widely used DNS implementations and public DNS providers. Exploitation of this attack would have severe consequences for any application using the Internet including unavailability of technologies such as web-browsing, e-mail, and instant messaging. With KeyTrap, an attacker could completely disable large parts of the worldwide Internet.The researchers worked with all relevant vendors and major public DNS providers over several months, resulting in a number of vendor-specific patches, the last ones published on Tuesday, February 13. It is highly recommended for all providers of DNS services to apply these patches immediately to mitigate this critical vulnerability.

Researchers from the National Research Center for Applied Cybersecurity ATHENE in Darmstadt and Frankfurt, Germany, have uncovered a critical flaw in the design of DNSSEC (DNS Security Extensions) which introduces a vulnerability in all DNS (Domain Name System) implementations. The team consisting of Prof. Dr. Haya Schulmann and Niklas Vogel, both from Goethe University Frankfurt, Elias Heftrig from Fraunhofer SIT and Prof. Dr. Michael Waidner from Technical University of Darmstadt and Fraunhofer SIT developed a new class of so-called Algorithmic Complexity Attacks, which they dubbed "KeyTrap". They demonstrated that just with a single DNS packet the attack can exhaust the CPU and stall all widely used DNS implementations and public DNS providers, such as Google Public DNS and Cloudflare. In fact, the popular Bind9 DNS implementation can be stalled for as long as 16 hours. This devastating effect prompted major DNS vendors to refer to KeyTrap as "The worst attack on DNS ever discovered". The impact of KeyTrap attacks is far reaching. Exploiting KeyTrap attackers can effectively disable Internet access in any system utilizing a DNSSEC-validating DNS resolver.

The attack vectors exploited in the KeyTrap class of attacks are registered in the Common Vulnerabilities and Exposures (CVE) database as an umbrella CVE-2023-50387.

DNS evolved into a fundamental system in the Internet that underlies a wide range of applications and facilitates new and emerging technologies. Recent measurements show that in December 2023, 31.47% of the web clients worldwide used DNSSEC-validating DNS resolvers. Therefore, the KeyTrap attacks affect not only DNS but also any application using it. An unavailability of DNS may not only prevent access to content but risks also disabling security mechanisms, like anti-spam defenses, Public Key Infrastructures (PKI), or even inter-domain routing security like RPKI (Resource Public Key Infrastructure).

The flaws are not recent. The vulnerable requirements were present already in the obsoleted Internet standard RFC 2535 from 1999. In 2012 the vulnerability made its way into the implementation requirements for DNSSEC validation, standards RFC 6781

and RFC 6840. The vulnerabilities have been in the wild since at least August 2000 in the Bind9 DNS resolver and were introduced into the code of the Unbound DNS resolver in August 2007. Although the vulnerabilities have existed in the standard for about 25 years and in the wild for 24 years, they have not been noticed by the community. This is not surprising since the complexity of the DNSSEC validation requirements made it challenging to identify the flaws. The exploit requires a combination of a number of requirements, which made it not trivial even for DNS experts to notice. The security community made similar experiences with much simpler vulnerabilities, such as Heartbleed or Log4j, which were there but no one could see them, and they took years to notice and fix. Unfortunately, in contrast to these vulnerabilities, the vulnerabilities the ATHENE team identified are not simple to resolve, since they are fundamentally rooted in the design philosophy of DNSSEC, and are not just mere software implementation bugs. Since the initial disclosure of the vulnerabilities, the team has been working with all major vendors on mitigating the problems in their implementations, but it seems that completely preventing the attacks requires to fundamentally reconsider the underlying design philosophy of DNSSEC, i.e., to revise the DNSSEC standards.

The National Research Center for Applied Cybersecurity ATHENE is a research center of Fraunhofer-Gesellschaft that brings together the Fraunhofer Institutes for Secure Information Technology (SIT) and for Computer Graphics Research (IGD), Technical University of Darmstadt, Goethe University Frankfurt, and Darmstadt University of Applied Sciences. With more than 600 scientists, ATHENE is the largest cybersecurity research center in Europe and Germany's leading scientific research institution in this domain.

Contact:

Cornelia Reitz

cornelia.reitz@athene-center.de

+49 6151 869-213 or +49 6151 869-368

Medieninhalte

The National Research Center for Applied Cybersecurity ATHENE has uncovered a critical flaw in the design of DNSSEC, the Security Extensions of DNS (Domain Name System). DNS is one of the fundamental building blocks of the Internet. / More information via ots and www.presseportal.de/en/nr/173495 / The use of this image for editorial purposes is permitted and free of charge provided that all conditions of use are complied with. Publication must include image credits.