11.04.2024 – 16:41 Uhr

Severe Vulnerabilities Discovered in Software to Protect Internet Routing

Frankfurt and Darmstadt (ots) -

A research team from the National Research Center for Applied Cybersecurity ATHENE led by Prof. Dr. Haya Schulmann has uncovered 18 vulnerabilities in crucial software components of Resource Public Key Infrastructure (RPKI). RPKI is an Internet standard meant to protect Internet traffic from being hijacked by hackers. By now, all affected vendors provided patches for their products. The vulnerabilities could have had devastating consequences: Internet hijacks have already been exploited, e.g., for phishing passwords and other sensitive information, tricking certificate authorities into issuing fraudulent Web certificates, stealing cryptocurrency, distributing malware, and poisoning caches of DNS servers.

The ATHENE team consisting of Prof. Dr. Haya Schulmann and Niklas Vogel, both from Goethe University of Frankfurt, Donika Mirdita from TU Darmstadt, and Prof. Dr. Michael Waidner from TU Darmstadt and Fraunhofer SIT uncovered and disclosed 18 vulnerabilities. The National Vulnerability Database (NVD), operated by the US National Institute of Standards and Technology (NIST), assigned five Common Vulnerabilities and Exposures (CVE) entries to these vulnerabilities, some critical with a score of 9.3 out of 10. The team used a testing tool, CURE, which they developed specifically for this project and which ATHENE makes available free of charge to all developers of RPKI software. The researchers found vulnerabilities in all popular implementations of the validator component of RPKI. They range between crashes, violation of standard behavior, and even severe bugs that allow a network adversary to completely take over an RPKI certificate hierarchy in order to inject its own trust anchor - effectively being able to forge authentic and valid yet bogus routing information (i.e., BGP announcements). It is unknown whether any of the vulnerabilities were already exploited by hackers in the wild.

RPKI is a relatively new standard. Today, about 50% of the Internet's network prefixes are covered by RPKI certificates, and 37.8% of all Internet domains validate RPKI certificates. In particular, many large providers and operators support RPKI, e.g., Amazon Web Services, Cogent, Deutsche Telekom, Level 3, and Zayo.

The research work was carried out in the ATHENE research area Analytic Based Cybersecurity (ABC) (more information at https://abc.athene-center.de/en/) and appeared at the 2024 Network and Distributed System Security (NDSS) Symposium in San Diego, California, USA. The research paper can be downloaded from https://www.ndss-symposium.org/ndss-paper/the-cure-to-vulnerabilities-in-rpki-validation/. The testing tool CURE developed and used by the researchers to uncover the vulnerabilities can be downloaded from https://github.com/rp-cure/rp-cure.

The **National Research Center for Applied Cybersecurity ATHENE** is a research center of the Fraunhofer Society that brings together the Fraunhofer Institutes for Secure Information Technology (SIT) and for Computer Graphics Research (IGD), Technische Universität Darmstadt, Goethe-Universität Frankfurt am Main, and Darmstadt University of Applied Sciences. With more than 600 scientists, ATHENE is Europe's most prominent cybersecurity research center and Germany's leading scientific research institution in this domain. ATHENE is supported by the German Federal Ministry of Education and Research (BMBF) and the Hessian Ministry for Higher Education, Research, Science and the Arts (HMWK). Further information about ATHENE can be found at https://www.athene-center.de/en/.

Press Contact:

Mrs. Cornelia Reitz, cornelia.reitz@athene-center.de

Medieninhalte

The vulnerabilities could have had devastating consequences: Internet hijacks have already been exploited, e.g., for phishing passwords and other sensitive information, tricking certifi-cate authorities into issuing fraudulent Web certificates, stealing cryptocurrency, distributing malware, and poisoning caches of DNS servers. / 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.

Original content of: National Research Center for Applied Cybersecurity ATHENE, transmitted by news aktuell
Diese Meldung kann unter https://www.presseportal.de/en/pm/173495/5755440 abgerufen werden.