Public Review for

On the Potential Abuse of IGMP

Matthew Sargent, John Kristoff, Vern Paxson, Mark Allman

Dear readers, welcome to another episode of our series named *"Oh, if only we had security in mind when we designed connectionless protocols!"*.
In its April 2016 issue, CCR featured a paper about vulnerabilities in NTP, a protocol that has been around for a long time. This time, a different group of authors addresses a vulnerability of another ancient Internet protocol: the Internet Group Management Protocol (IGMP), which allows neighboring hosts and routers to exchange multicast membership status information.
Like the authors of the mentioned NTP paper, Sargent et al. perform a survey of the IPv4 address space to identify vulnerable systems, IGMP responders in this case. However, the vulnerability discussed and analyzed in this paper does not affect functionalities for which the protocol itself was designed, but rather allows an attacker to mount reflective DoS attacks. The severity of this vulnerability is magnified by the amplification opportunities it offers: the authors find that 1% of the responding routers generate responses that are at least 100 times larger than the requests. In other words, the attacker not only can hide behind spoofed addresses but can also "pay less for more", in terms of bandwidth used versus bandwidth of the actual DoS traffic. To conclude the list of analogies with the previous paper of our mini series, the authors informed vendors early, to allow them time to address this issue.
CCR reviewers noted that the number of vulnerable routers is relatively small compared to other vulnerabilities, such as DNS open resolvers, but the opportunity for attackers is undeniable. Reviewers found the paper enjoyable to read, they appreciated the extensive measurements and characterization of vulnerable hosts to gain insight. Finally, for the sake of repeatability, replicability & reproducibility, the editors considered requesting that the authors release the Zmap module they developed and the raw data of their IPv4 survey. However, we concluded that public release of this data may cause harm, and decided to leave to the authors the responsibility of vetting researchers who may want to access data and tools from this paper for their own experiments.
Enjoy your reading, and stay tuned for the next episode (..or hopefully not).

Public review written by
Alberto Dainotti
CAIDA, UC San Diego