What is open recursive DNS and why is it risky?

What is open recursive DNS and why is it risky?

Context

You may have received a notice from the security team with the following information:

A machine registered to you, or in your area of responsibility, has been identified as running an open recursive DNS resolver that is accessible from outside of MIT: (example) MACHINE.MIT.EDU [18.187.1.203]

Answer

Why is this a concern?

There are a few reasons. If recursion is not needed or used, running it can be a liability. Additionally, as this server is an open recursive DNS resolver, it's susceptible to abuse, often leveraged in denial-of-service attacks (what's called DNS amplification). Denial of Service attacks can have an impact on network reliability. "A DNS resolver is open if it provides recursive name resolution for clients outside of its administrative domain."[1]

Additional information about the dangers of open DNS resolvers can be found below [2].

Recommendation

Review the configuration and decide if recursion on these name servers can be disabled as described in section 4 of RFC-5358 [3]. Before you disable recursion you will need to assess the implications and impact to your environment and users.

If you feel that recursion isn't a necessary component, it may be prudent to disable it. If it is necessary, you may want to configure it to respond to only local queries from machines you trust.

The information below provides steps on how to securely deploy BIND and Windows DNS.

Additional information

If you have questions about the notice you received from Security Operations, contact them at security@mit.edu. For additional help, contact the Help Desk at helpdesk@mit.edu.

[1] DNS SURVEY: OPEN RESOLVERS
http://dns.measurement-factory.com/surveys/openresolvers.html

[2] The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)

[3] RFC-5358 - Preventing Use of Recursive Nameservers in Reflector Attacks
http://www.ietf.org/rfc/rfc5358.txt

Other resources:

Team Cymru - Secure BIND Template Version
http://www.cymru.com/Documents/secure-bind-template.html

Deploying Secure DNS

Mitigating DNS Denial of Service Attacks
https://www.dns-oarc.net/wiki/mitigating-dns-denial-of-service-attacks

The Million Plus Open Resolver Challenge