Network Working Group E. Gavron Request for Comments: 1535
ACES Research Inc. Category: Informational October 1993

A Security Problem and Proposed Correction With Widely Deployed DNS Software

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Abstract

This document discusses a flaw in some of the currently distributed name resolver clients. The flaw exposes a security weakness related to the search heuristic invoked by these same resolvers when users provide a partial domain name, and which is easy to exploit (although not by the masses). This document points out the flaw, a case in point, and a solution.

Background

Current Domain Name Server clients are designed to ease the burden of remembering IP dotted quad addresses. As such they translate human- readable names into addresses and other resource records. Part of the translation process includes understanding and dealing with hostnames that are not fully qualified domain names (FQDNs).

An absolute "rooted" FQDN is of the format {name}{.} A non "rooted" domain name is of the format {name}

A domain name may have many parts and typically these include the host, domain, and type. Example: foobar.company.com or fooschool.university.edu.

Flaw

The problem with most widely distributed resolvers based on the BSD BIND resolver is that they attempt to resolve a partial name by processing a search list of partial domains to be added to portions of the specified host name until a DNS record is found. This "feature" is disabled by default in the official BIND 4.9.2 release.

Example: A TELNET attempt by User@Machine.Tech.ACES.COM to UnivHost.University.EDU

The resolver client will realize that since "UnivHost.University.EDU" does not end with a ".", it is not an absolute "rooted" FQDN. It will then try the following combinations until a resource record is found:

UnivHost.University.EDU.Tech.ACES.COM.
UnivHost.University.EDU.ACES.COM. UnivHost.University.EDU.COM.
UnivHost.University.EDU.

Security Issue

After registering the EDU.COM domain, it was discovered that an unliberal application of one wildcard CNAME record would cause *all* connects from any .COM site to any .EDU site to terminate at one target machine in the private edu.com sub-domain.

Further, discussion reveals that specific hostnames registered in this private subdomain, or any similarly named subdomain may be used to spoof a host.

Example: harvard.edu.com. CNAME targethost

Thus all connects to Harvard.edu from all .com sites would end up at targthost, a machine which could provide a Harvard.edu login banner.

This is clearly unacceptable. Further, it could only be made worse with domains like COM.EDU, MIL.GOV, GOV.COM, etc.

Public vs. Local Name Space Administration

The specification of the Domain Name System and the software that implements it provides an undifferentiated hierarchy which permits delegation of administration for subordinate portions of the name space. Actual administration of the name space is divided between "public" and "local" portions. Public administration pertains to all top-level domains, such as .COM and .EDU. For some domains, it also pertains to some number of sub-domain levels. The multi-level nature of the public administration is most evident for top-level domains for countries. For example in the Fully Qualified Domain Name, dbc.mtview.ca.us., the portion "mtview.ca.us" represents three levels of public administration. Only the left-most portion is subject to local administration.

The danger of the heuristic search common in current practise is that it it is possible to "intercept" the search by matching against an unintended value while walking up the search list. While this is potentially dangerous at any level, it is entirely unacceptable when the error impacts users outside of a local administration.

When attempting to resolve a partial domain name, DNS resolvers use the Domain Name of the searching host for deriving the search list. Existing DNS resolvers do not distinguish the portion of that name which is in the locally administered scope from the part that is publically administered.

Solution(s)

At a minimum, DNS resolvers must honor the BOUNDARY between local and public administration, by limiting any search lists to locally- administered portions of the Domain Name space. This requires a parameter which shows the scope of the name space controlled by the local administrator.

This would permit progressive searches from the most qualified to less qualified up through the locally controlled domain, but not beyond.

For example, if the local user were trying to reach:

User@chief.admin.DESERTU.EDU from starburst,astro.DESERTU.EDU,

it is reasonable to permit the user to enter just chief.admin, and for the search to cover:

chief.admin.astro.DESERTU.EDU chief.admin.DESERTU.EDU

but not

chief.admin.EDU

In this case, the value of "search" should be set to "DESERTU.EDU" because that's the scope of the name space controlled by the local DNS administrator.

This is more than a mere optimization hack. The local administrator has control over the assignment of names within the locally administered domain, so the administrator can make sure that abbreviations result in the right thing. Outside of the local control, users are necessarily at risk.

A more stringent mechanism is implemented in BIND 4.9.2, to respond to this problem:

The DNS Name resolver clients narrows its IMPLICIT search list IF ANY to only try the first and the last of the examples shown.

Any additional search alternatives must be configured into the resolver EXPLICITLY.

DNS Name resolver software SHOULD NOT use implicit search lists in attempts to resolve partial names into absolute FQDNs other than the hosts's immediate parent domain.

Resolvers which continue to use implicit search lists MUST limit their scope to locally administered sub-domains.

DNS Name resolver software SHOULD NOT come pre-configured with explicit search lists that perpetuate this problem.

Further, in any event where a "." exists in a specified name it should be assumed to be a fully qualified domain name (FQDN) and SHOULD be tried as a rooted name first.

Example: Given user@a.b.c.d connecting to e.f.g.h only two tries should be attempted as a result of using an implicit search list:

e.f.g.h. and e.f.g.h.b.c.d.

Given user@a.b.c.d. connecting to host those same two tries would appear as:

x.b.c.d. and x.

Some organizations make regular use of multi-part, partially qualified Domain Names. For example, host foo.loc1.org.city.state.us might be used to making references to bar.loc2, or mumble.loc3, all of which refer to whatever.locN.org.city.state.us

The stringent implicit search rules for BIND 4.9.2 will now cause these searches to fail. To return the ability for them to succeed, configuration of the client resolvers must be changed to include an explicit search rule for org.city.state.us. That is, it must contain an explicit rule for any -- and each -- portion of the locally- administered sub-domain that it wishes to have as part of the search list.

References

[1] Mockapetris, P., "Domain Names Concepts and Facilities", STD 13, RFC 1034, USC/Information Sciences Institute, November 1987.

[2] Mockapetris, P., "Domain Names Implementation and Specification", STD 13, RFC 1035, USC/Information Sciences Institute, November 1987.

[3] Partridge, C., "Mail Routing and the Domain System", STD 14, RFC 974, CSNET CIC BBN, January 1986.

[4] Kumar, A., Postel, J., Neuman, C., Danzig, P., and S. Miller, "Common DNS Implementation Errors and Suggested Fixes", RFC 1536, USC/Information Sciences Institute, USC, October 1993.

[5] Beertema, P., "Common DNS Data File Configuration Errors", RFC 1537, CWI, October 1993.

Security Considerations

This memo indicates vulnerabilities with all too-forgiving DNS clients. It points out a correction that would eliminate the future potential of the problem.

Author's Address

Ehud Gavron ACES Research Inc. PO Box 14546 Tucson, AZ 85711

Phone: (602) 743-9841 EMail: gavron@aces.com