Immunity, Inc. Member's Only Advisory

Disclosure

This advisory has been released and may be redistributed in full. Other use is prohibited.

Vulnerability

Remote double-free vulnerability in dtlogin (part of CDE)

dtlogin is the process on Solaris (and presumably HP-UX, AIX, and other Unixes which support CDE) which implements the XDMCPD protocol. This protocol is what is used when you call X -query host:port. It runs over UDP port 177. The vulnerability is available before any authentication, and XDMCPD is turned on by default. Dtlogin runs as root. This vulnerability is known to be exploitable, although it's not an easy exploit to write.

Affected

Solaris 8 is known to be affected. Other Solaris's and other Unix's (not Linux, however) are also most likely vulnerable.

Detection

Immunity has released a SPIKE script as part of The Shellcoder's Handbook which replicates this vulnerability, in addition to a Python script which crashes dtlogin.

There is currently no known patch for this vulnerability.

For questions or comments, please contact Immunity, Inc. at dave@immunitysec.com, or http://www.immunitysec.com.

History

Found by Immunity Researcher Dave Aitel June 6, 2002