Immunity, Inc. Advisory

Disclosure

This advisory is has been released to the public, and may be retransmitted without modification.

Vulnerability

Remote, unauthenticated stack overflow Computer Associates Unicenter TNG Utilities awservices.exe

Computer Associates has developed a suite of tools that help enterprises manage the software on their machines. In doing so, they developed several proprietary protocols, which are implemented in various daemons, listening on TCP and UDP ports, and running as SYSTEM. These daemons are vulnerable to classic stack overflows. In particular, Immunity reviewed cam.exe and awservices.exe, and found many examples of exploitable problems in both. These are considered critical problems, as they are often installed on every machine in an enterprise.

These bugs are exploitable, but are one-shots, and require knowledge of the Windows version to be effective in some cases. If these processes exit, they will leave an event log.

It should be noted that strcpy() and strcat() are used heavily. Other, similar, problems are no doubt evident many other services in Unicenter. If you use Unicenter, it is recommended you receive a source code audit of it from a security vendor you trust.

Affected

All known versions of Unicenter TNG 2.4 are affected. According to Computer Associates, this problem was previously fixed in TNG 2.5

Detection

Immunity Research has provided working exploits for these problems. (See your CANVAS distribution)

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

History

Found by Immunity Researcher Dave Aitel, October-December, 2003.