1400 - Call the plumber - you have a leak in your (named) pipe

Sunday at 14:00 in 101 Track
45 minutes | Demo
Gil Cohen*CTO, Comsec group*

The typical security professional is largely unfamiliar with the Windows named pipes interface, or considers it to be an internal-only communication interface.
As a result, open RPC (135) or SMB (445) ports are typically considered potentially entry points in "infrastructure" penetration tests.

However, named pipes can in fact be used as an application-level entry vector for well known attacks such as buffer overflow, denial of service or even code injection attacks and XML bombs, depending on the nature of listening service to the specific pipe on the target machine.

As it turns out, it seems that many popular and widely used Microsoft Windows-based enterprise applications open a large number of named pipes on each endpoint or server on which they are deployed, significantly increase an environment's attack surface without the organization or end user being aware of the risk.
Since there's a complete lack of awareness to the entry point, there's very limited options available to organizations to mitigate it, making it a perfect attack target for the sophisticated attacker.

In this presentation we will highlight how named pipes have become a neglected and forgotten external interface. We will show some tools that can help find vulnerable named pipes, discuss the mitigations, and demonstrate the exploitation process on a vulnerable interface.
Gil Cohen
Gil is an experienced application security instructor, architect, consultant and pentester just starting his 12th year in the field.

With past experience in the civilian, government and military cyber security industries, Gil currently serves as the CTO of Comsec Group, in charge of training, research, service lines, methodologies and quality assurance.

With a long time record as an SQL injection fanatic, Gil was responsible for publishing the

"SQL Injection Anywhere" technique in 2010, which is currently in use in a variety of automated scanners in the market, and enables the blind detection and exploitation of potential injections in any part of the SQL statement.

He also has a taste for nostalgia, and has been working for a while on abuses to protocols that software developers would prefer to forget.

@Gilco83
www.facebook.com/gilc83

#defcon25/by_track/101/Sunday #defcon25/By_Day/_Sunday