

The Evolution of an Exploit

Wednesday, 24th June 2009

A half day event, hosted by MWR InfoSecurity,
St Clement House, 1-3 Alencon Link, Basingstoke, RG21 7SB

The workshop is aimed at uncovering some of the mystery and uncertainty that can surround the subject of vulnerability discovery and exploit development. However, to understand them at a high level it is necessary to explore them at a fairly detailed technical level. The workshop will include background on areas such as interpreting and constructing code, how memory addressing works and assembly level programming - these subjects can require a steep learning curve without prior experience of them. Therefore, whilst the workshop is open to people with all levels of technical knowledge an attendee should expect to find the course material challenging, particularly without recent experience of the relevant technical areas. Attendees should also be aware that technically focused practical exercises are planned for the session and are typically solved in small teams formed amongst the attendees.

REGISTRATION, 10.00 – 10.45

11.00am - The Evolution of an Exploit - Martyn Ruks, Rafael Dominguez-Vega

The half day session will be highly focused, and will guide the attendees through the process used to identify and exploit vulnerabilities across a variety of technologies. We will use a number of recent vulnerabilities discovered by MWR InfoSecurity as examples.

The discovery and evolution of an exploit can be broken in to a number of areas. The sessions will cover and demonstrate the techniques used in the following areas:

- Product Investigation
- Protocol Fuzzing
- Crash Analysis
- Vulnerability Identification
- Exploit authoring and Exploitation

The MWR InfoSecurity team will use an interactive style to demonstrate many of these areas, allowing the transfer of knowledge necessary to evaluate risk in new products through an understanding of the technical examination techniques utilised.

At the end of the session we hope that attendees will have a better understanding of how exploits can be identified, what approach to take when investigating, and how this can help in assessing threats and risk in the context of your organisation.

There will be light lunch at 1.00pm and the session will finish at approximately 3.30pm

Numbers for this session will be limited to 10.

Please confirm your interest to John.Dixon@mwrinfosecurity.com