Detecting the Baron Samedit sudo attack

Scenario: The buffer overflow attack dubbed Baron Samedit can result in privilege escalations on some of the most modern and widely used Linux operating systems. An unprivileged user can exploit this vulnerability to gain root privileges on a host by using a default sudo configuration. You have Linux and Unix machines in your network and those machines have the sudo command. You need a proactive way to interrogate your servers and make a data-driven response to manage your threat surface.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: System administrator
- Technologies:
  - Splunk Enterprise or Splunk Cloud Platform
  - Add-on for OSquery
  - Splunk Add-on for Unix and Linux
  - Technical Add-on for Samedit
- Data: *nix logs

How to use Splunk software for this use case

Depending on what information you have available, you might find it useful to identify some or all of the following:

- Active detection of Baron Samedit vulnerabilities
- Heap-based buffer overflow on *nix

Results

These searches give you a proactive way to interrogate your servers and make a data-driven response to manage your threat surface.

Additional resources

The content in this use case comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement this specific use case:
• Conf Presentation: ATT&CKing Linux using SPL
• Blog: Hunting with Splunk: The Basics (this is a series starting from this link)