



Skyjacking and zero-day vulnerabilities

Are you ready?

Skyjacking

The latest vulnerability “Skyjacking” of Cisco lightweight access points (LAPs) is a prime example of a zero-day vulnerability that can leave enterprise networks exposed and at the mercy of hackers. It is also a reminder that having a second line of defense independent of your infrastructure is the best way forward for proactively securing your network and data against zero-day attacks.

	Skyjacking	Other wireless zero-day vulnerabilities
SpectraGuard® Enterprise <ul style="list-style-type: none">▪ Patented marker packet technology and unique VLAN Policy Mapping™ architecture makes it the only wireless intrusion prevention system (WIPS) that can detect and protect against the most lethal exploits of skyjacking▪ Serves as a second line of defense to protect an enterprise network against zero-day attacks, undesirable connections, and misconfigurations that otherwise can go undetected.	✓	✓
Block firewall ports <ul style="list-style-type: none">▪ Blocking UDP ports 12222 and 12223 used by Cisco LWAP can protect against skyjacking by a remote attacker.▪ But this is not a common practice. Administrators often rely on content filters instead of defining port blocking rules on a firewall as managing numerous rules can become a nightmare.	✓	X
Configure LSC <ul style="list-style-type: none">▪ Manually configuring the wireless controller (WLC) and all LAPs with locally significant certificates (LSC) can protect against skyjacking.▪ However this is rarely put into practice as it is painstaking for any reasonable-sized wireless LAN.	✓	X
Configure preferred WLC <ul style="list-style-type: none">▪ Manually configuring each LAP with primary, secondary, and tertiary WLC will make the LAPs to first look for one of the preferred WLC for connection. This will reduce the likelihood of a LAP getting skyjacked.▪ However, this is primarily a high availability and load balancing feature and does not guarantee security. If a LAP loses connection with its list of preferred WLCs, then it can still be skyjacked.	~	X