

AS-Path prepending can be good way of directing traffic easily and simply through a router. But in some cases, human error can allow prepending to take down thousands of devices. One of these instances occurred when a user accidentally prepended all AS-paths coming through the router 255 times which crashed certain Cisco routers at the time, which caused a huge outage. Also, a huge vulnerability is some companies are using excessive prepending in a way that a hijacker could easily impersonate the AS. They do this by advertising the same path with not as many prepended paths, this would trick routers into thinking it is the same path just more desirable. This type of intrusion becomes more of a reality when the amount of ipv4/6 prepending to all route tables are increasing at a stable rate every year. This then raises the questions of why prepend at all? A first theory could just be bad housekeeping, maybe in the past NetOps wanted to easily control traffic throughout their network and never found a better way to do it or it just never changed while other aspects of the network did. Another theory could just be human error like I briefly mentioned before. Overall this video taught me that long AS paths create security risks and that operators should think if prepending is absolutely necessary before implementing it.