SearchSecurity.com

DHCP servers must be patched against denial-of-service attacks

By null

The Internet Systems Consortium has patched a flaw in the Dynamic Host Configuration Protocol that could lead to denial-of-service attacks, but experts were split on whether this issue should lead organizations to switch to IPv6.

According to the advisory released by Internet Systems Consortium (ISC), the vulnerability puts "nearly all IPv4 Dynamic Host Configuration Protocol (DHCP) clients and relays, and most IPv4 DHCP servers" at risk. If an attacker were to send a badly formed packet with an invalid IPv4 UDP length field, it could cause a DHCP server, client or relay program to terminate abnormally.

Stephen Gates, principal sales engineer and technical expert from network security firm NSFOCUS IB, said this vulnerability is likely not able to be exploited from outside of an enterprise network.

"More often, this denial-of-service attack would be launched by an internal machine attacking a DHCP server from the inside," Gates said. "For example, in a cable operator's network, a rogue client machine could attack one of the cable operator's DHCP servers, rendering it unavailable for any other clients on that portion of the network. That would not be a good situation for anyone."

ISC said that it would be difficult to test whether or not a DHCP build would be affected, so it suggests all builds be considered vulnerable and upgraded. ISC also noted that while there are no mitigation techniques available, exposure to attacks can be limited by "configuring firewalls to block inbound requests to the DHCP server except for those that come from authorized relay agents or directly-served subnets."

ISC advised organizations to upgrade immediately to DHCP version 4.1-ESV-R12-P1 or DHCP version 4.3.3-P1.

Experts agreed that switching to IPv6 would also allow enterprises to avoid the issue because DHCPv6 is a "stateless DHCP" and would not be exposed to the same flaw. However, experts were split on whether the cost and work to transition to IPv6 would be worthwhile.

Some, like Andrew Lewman, senior vice president of engineering at threat intelligence company Norse Corp., said IPv6 is the future of networking and all enterprises should plan to migrate, but others disagreed.

Tom Gorup, security operations leader at managed security service provider Rook Security, said the transition isn't a pressing issue because "you won't be running out of IPv4 addresses on your internal network anytime soon."

Garve Hays, solutions architect at software vendor Micro Focus, said it would come down to an economic choice because the cost to migrate to IPv6 would be "much greater" than upgrading DHCP clients and relays.

"IPv6 packets are much larger than IPv4 ones (128-bit vs 32-bit)," Hays said, "which may require the

purchase of new networking equipment. Furthermore, there may be issues of compatibility with partners or Internet service providers."

18 Jan 2016