USE CASE

Identify Log4Shell Exposure In Seconds

Discovered on December 9, 2021 by Minecraft players, the Apache Log4Shell vulnerability enables bad actors using text-based chats to gain ACE access to your system, plant malware, and download anything internet accessible from the compromised host. Security experts predict that this vulnerability will “haunt the internet for years” because it’s incredibly difficult to ensure that all infected devices are remediated.

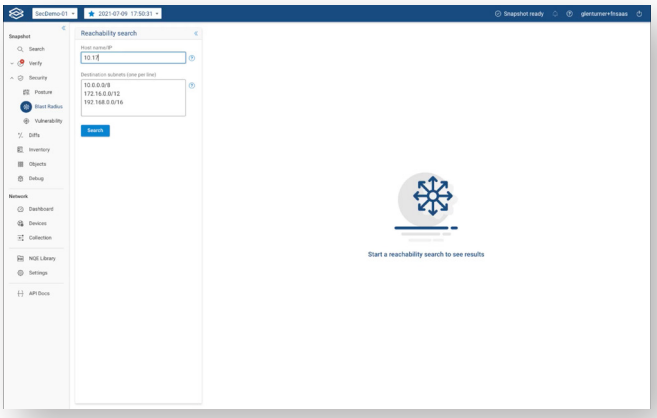
To truly protect your organization from Log4Shell, you need to know with mathematical certainty every device that could have communicated with an infected host. Which is to say, you need to know how your exposure has changed over time. For most agencies, it’s an arduous and time-consuming task to determine which devices are currently within the blast radius, and it would be impossible to construct an inventory of potential exposure over time.

The Forward Enterprise blast radius feature was engineered to provide detailed, actionable data on the exposure created by an infected host so that time isn’t wasted searching for information and the risk of overlooking at-risk devices is virtually eliminated.

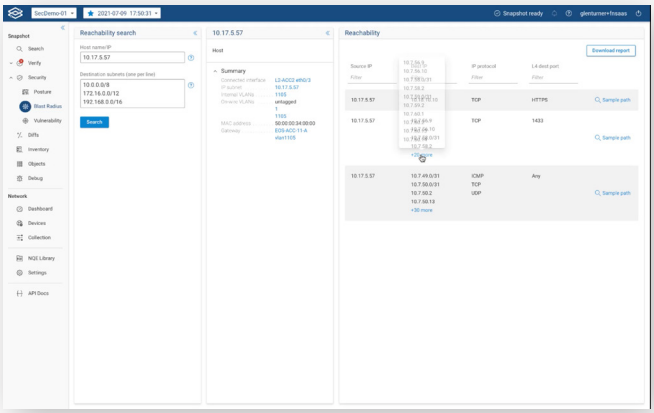
Forward Enterprise users can create an accurate report of current exposure in seconds. Combining the power of network snapshots with our blast radius feature provides an accurate audit of all potential past and present exposure that ops teams can use to construct a forensic investigation and remediate the vulnerability.

Because all members of the team are working from an intuitive single source of truth, their time is spent effectively remediating exposure instead of performing time-consuming manual path searches.

Identifying and isolating impacted devices is a 3-step process.



STEP 1:
Select the Blast Radius feature under the security tab, and input the hostname of the compromised device and any destination IP addresses that may be of interest. Then click on the blast radius button.



STEP 2:
View a comprehensive table and all possible flows from the host to the destination subnets, including protocol and L4 destination port. In a single click, you can download a report that documents the blast radius.

STEP 3:
Track the blast radius exposure over time using snapshots.

See it in Action

If this sounds too good to be true, give us 30 minutes and we'll show exactly how easy it is.

Request a personal demo ›

FORWARD NETWORKS

www.forwardnetworks.com