Log4Shell Compromise Assessment

World-Class Investigative Expertise to Identify the Log4Shell Vulnerability, Hunt for Threats, and Reduce Uncertainty

Benefits of a Log4Shell Compromise Assessment

- Understand and manage your Log4Shell risk.
- Identify red flags indicating potential compromise.
- Detect hidden cybersecurity threats.

What Is the Log4Shell Vulnerability?

The Log4Shell vulnerability, also known as Log4j, is a remote code execution (RCE) vulnerability in Apache log4j 2. Many Java-based applications use log4j as their logging utility and are vulnerable if not properly patched. Exploitation of this vulnerability is easy and could allow a vulnerable system to download and execute a malicious payload. Activities that could be attempted include mass scanning, vulnerable server discovery, information stealing, and possible delivery of backdoors or other unauthorized software.

Impacted Java-based applications are widely used on corporate and home networks, making this a high-risk vulnerability now and in the future. For more information, read the Unit 42 blog, Another Apache Log4j Vulnerability Is Actively Exploited in the Wild.

Our Approach to Compromise Assessments

Comprehensive methodology: Focused and detailed, our assessment provides transparency to your organization, identifies potential red flags, and highlights hidden risks. Unit 42 incident response experts will provide an independent appraisal of in-scope assets, performing sweeps focused on identifying malicious threat actor behaviors and malicious IoCs.

Threat intelligence: We understand threats and trends targeting your industry, based on 200 threat researchers building insights from analyzing billions of events a day across endpoint, network, and cloud data from 85k customers. Specific to Log4Shell, hundreds of thousands of security experts have leveraged Unit 42's continuously updated threat analysis to guide their response efforts. We apply our threat intelligence and real-world investigative observations to customize a Log4Shell compromise assessment for your unique environment.

Leading technical and industry experience: The Unit 42 compromise assessment team is composed of seasoned incident response and threat hunting experts armed with best-in-class tools and threat intelligence. We support more than 1,000 incident response investigations per year across all major verticals, ranging from insider threats to nation-state APTs.

Identify the Hidden Risks Across Your Environment

When you undertake a Log4Shell compromise assessment with Unit 42, we will proactively search for historical and ongoing indicators of compromise to discover previously undetected malicious activity that may be occurring in your environment. This enables you to respond before any further damage occurs. We use a threat-informed approach, taking full advantage of Unit 42's extensive telemetry data from Palo Alto Networks cybersecurity products deployed worldwide, as well as the unique insights that can only be gained by working 1k+ incidents per year.

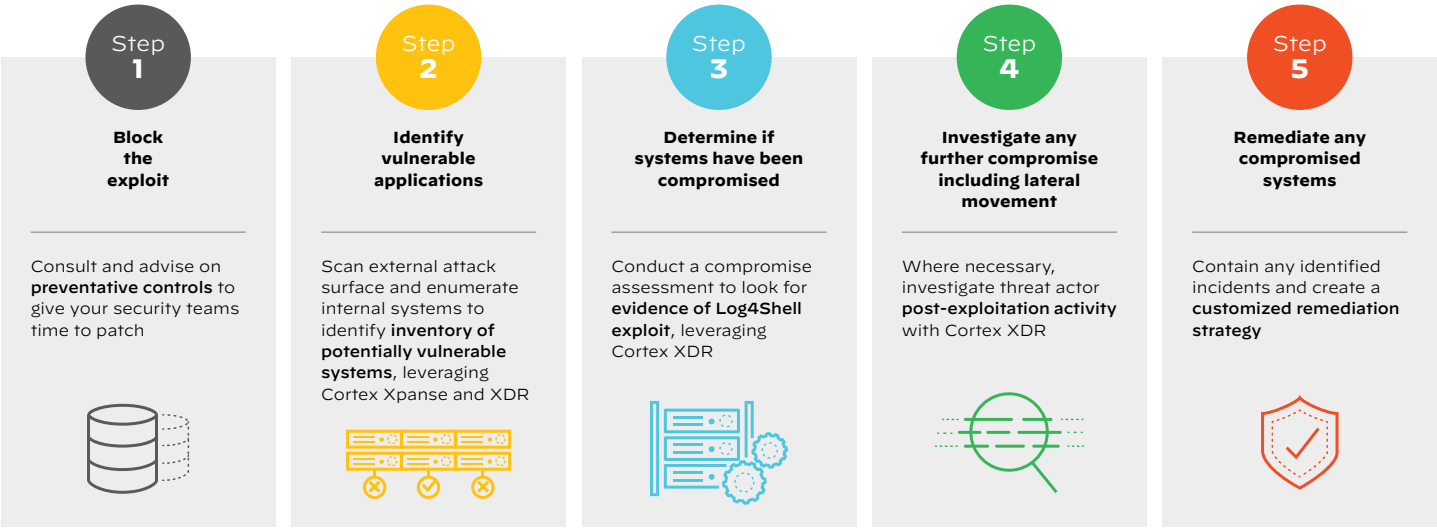

Figure 1: Unit 42's unique five-step approach helps you protect your organization

Approved by Cybersecurity Insurance Plans

Unit 42 is on the approved vendor panel of more than 70 major cybersecurity insurance carriers. If you need to use Unit 42 services in connection with a cyber insurance claim, Unit 42 can honor any applicable preferred panel rate in place with the insurance carrier. For the panel rate to apply, just inform Unit 42 at the time of the request for service.

Under Attack?

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team at start.paloaltonetworks.com/contact-unit42.html or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

About Unit 42

Palo Alto Networks Unit 42 brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk. With a deeply rooted reputation for delivering industry-leading threat intelligence, Unit 42 has expanded its scope to provide state-of-the-art incident response and cyber risk management services. Our consultants serve as your trusted advisor to assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time.

Visit paloaltonetworks.com/unit42.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

unit42_ds_log4shell_compromise-assessment_122921