Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Systemic Vulnerabilities in Information Technology—Log4Shell

Updated December 15, 2021

On December, 9, 2021 a critical vulnerability in software used by millions of internet servers was discovered. Since its discovery both criminals and nation-state actors have reportedly exploited it. This CRS Insight describes the vulnerability and considerations for federal government response.

Log4Shell

Log4j is an open-source tool the Apache Foundation makes available for logging web server activity. To do this, Log4J has to access many network services (e.g., network maps and directories). Malicious actors discovered a way to use the Log4j tool to send the servers commands that in turn gives them control of the servers. The cybersecurity community has named this vulnerability Log4Shell.

Log4Shell exploits have been observed throughout December. Some actors have used Log4Shell-hijacked servers to mine for cryptocurrencies and expand botnets.

Apache Foundation software is very useful and freely available, so it is widely used. Hundreds of software projects maintained by the foundation rely on volunteer developers and are supported by donations and sponsorships.

Current Responses

The Apache Foundation has released an updated version of Log4j which remediates the vulnerability. However, deploying this solution is not as straightforward as with other vulnerabilities (i.e., applying the patch).

1. Deploying the solution is logistically complex, as Log4j is not part of a single software platform. Instead it is a part of many different web services. Users will have to identify all instances of its use and in some cases recompile software using the patched version.
2. Vulnerable versions of the software go back nearly a decade, and some instances may be used in software that is no longer maintained.

Congressional Research Service
https://crsreports.congress.gov
IN11824

3. End users may not be aware that they are vulnerable because they are unaware that the web services they rely on use this tool. Some may have difficulty enumerating which servers and applications are vulnerable.

The private sector has taken several steps to minimize the exploitation of Log4Shell. Companies have produced security alerts to inform their customers and their broader community. Companies have updated their anti-malware programs to detect potential exploits of the vulnerability. Others have deployed rules to detect the types of queries that would compromise servers. Some have published mitigation guidance.

The federal government has also moved to mitigate this vulnerability. The Cybersecurity and Infrastructure Security Agency (CISA) published a statement on their efforts, including recommendations for asset owners. It is unclear how many federal and nonfederal entities are vulnerable. CISA is using the Joint Cyber Defense Collaborative (JCDC) to manage the incident. The creation of the JCDC executed a recommendation from the Cyberspace Solarium Commission and was enacted last year. In addition to the private sector, CISA is leveraging the Federal Bureau of Investigation and the National Security Agency in this response.

For federal agencies, CISA added Log4Shell to its *Known Exploited Vulnerabilities Catalog*. Per instructions in Binding Operational Directive 22-01, agencies have until December 24 to remediate the vulnerability in their systems, regardless of whether they are operated by the agency or by a third-party (e.g., a cloud service provider).

The White House has not disclosed whether it has activated a Cyber Unified Coordination Group or is using the National Cyber Incident Response Plan in this response, as it did during the SolarWinds response.

Options for Congress

This is not the first time the cybersecurity community has had to address this type of systemic vulnerability in information and communications technology. In 2014, government and private sector entities coordinated to resolve the Heartbleed bug. In that case too, the critical vulnerability existed in widely used open-source software. Lessons from that response are being applied to Log4Shell's response, but also highlight opportunities for policy changes.

Policymakers may choose to explore the creation of a specific capability to address systemic vulnerabilities in the future. The JCDC can support public and private sector actions to address Log4Shell. But the involvement of the JCDC does not activate new authorities, and remediation will rely on entities using their existing authorities and capabilities. Congress may choose to direct a federal agency to build a capability to assist the open source community in identifying and remediating vulnerabilities. Dedicated resources may help to alleviate some challenges that open source projects face, such as volunteer developers not being able to commit time to identifying and resolving security issues in the same way that corporate and proprietary software developers can. Once such capability may be to authorize an agency to proactively scan the internet to discover potentially vulnerable servers and notify their owners. CISA has a technical capability to do this, but their authority requires entities to request scanning. But, some may view this type of activity as unwanted, and it may trigger incident response teams at unaware organizations—procedures on capability use and limitations will need to be developed.

Additionally, policymakers may explore opportunities to strengthen public-private partnerships to address malicious actors exploiting vulnerabilities. The federal government and private companies have coordinated their actions to disrupt botnet operations in the past. However, the authority to do so is ad-hoc and entities frequently rely on court orders to empower them to move against malicious infrastructure. Some in Congress have proposed empowering agencies to take additional actions against malicious infrastructure. Policymakers may choose to examine what additional authorities may be granted to federal

agencies seeking to identify the infrastructure malicious actors use, conditions under which agencies may take action against that infrastructure, what options agencies may pursue (e.g., confiscating servers), and what protections private entities may have for assisting and partnering with agencies.

Policymakers may seek to create greater transparency in the software supply chain. When users acquire and deploy software, they may only be familiar with the end product and may be oblivious to the underlying components used to build that product. Policymakers may choose to enact proposals on software bills of materials (SBOMs) which would require software developers to disclose which software packages went into their final products. This transparency would speed up the discovery of potentially vulnerable information technology (IT). The federal government has recently required SBOMs for agency IT.

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer