# Lightstream Cyber Security

Flash Bulletin | March 24, 2022

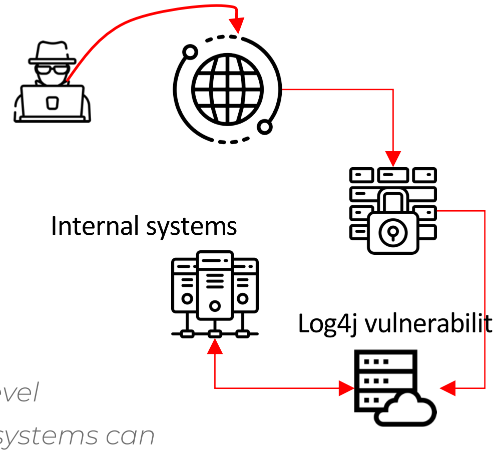
## Millions of Log4j vulnerable systems still unpatched

*A recent survey by Qualys and [published in SC Magazine](#) suggests that after over 3 months, roughly 1 in 3 devices and installations that were affected by the Log4j vulnerability are still unpatched. This number amounts to roughly 22 million vulnerable application installations – and it should be noted that these are just the devices that are readily accessible from the Internet.*

*Log4j reached critical status towards the end of 2021 when it was discovered that a feature its platform could allow an unauthenticated attacker to take complete control over a remote system. The vulnerability was classified in CVE-2021-44228, and has been extensively discussed in cyber security as well as in a published flash with guidance from the government's cyber security agency, CISA, [who published guidance](#).*

## Business Impact

*This Log4Shell vulnerability, as it's been colloquially named, impacts business systems exposed to the Internet (and systems connected to them) and can result in compromise of system and data integrity, as well as complete take-over of a system or platform generating severe operational and financial business impact.*



## Security Impact

*Using this vulnerability, attackers without credentials or otherwise legitimate access can exploit this weakness in Log4j to issue system-level commands, corrupting, disabling, or taking over a system. Subverted systems can then be used to deploy ransomware or attack protected, critical systems and exfiltrate sensitive data from organizations bypassing security controls.*

## Urgent Actions Required

1. *Scan all systems, on-premise and in the cloud, with a reliable vulnerability scanner*
2. *Triage all identified vulnerabilities, prioritize internet-accessible systems and connected devices*
3. *Patch Log4j vulnerabilities with the highest priority – closing any open vulnerabilities*

## Recommendations

*Lightstream recommends operating a comprehensive vulnerability management program and prioritizing issues like Log4j vulnerabilities as business-critical fixes.*

*If your organization does not have a functional vulnerability management program, Lightstream can help – we operate full-stack vulnerability management programs for our customers, keeping you ahead of emerging threats and attackers.*

### References

- *CISA guidance:*
- *SC Magazine reference:*
- *NIST reference:*