

To Our CISO Graylog Open Community Members,

First, thank you for choosing Graylog.

This is a courtesy notice from the team at Graylog. If you are running Graylog open-source deployments running outdated and unsupported versions of our software, please be aware that your older Graylog versions (before v3.0+) are susceptible to critical vulnerabilities, such as the Log4j/Log4Shell CVE ([CVE-2021-44228](#)) in December 2021.

For security reasons, we strongly suggest you update to the latest version, Graylog v5.0. In the newer versions of Graylog (after 3.0+), we have made regular bug fixes and feature enhancements, critical vulnerabilities, and security patches to ensure its security, including the Log4j/Log4Shell CVE ([CVE-2021-44228](#)) in December 2021.

Full changelog details can be found at the following links:

- Versions 3.3.0 (released 2020-05-20) and after
<https://docs.graylog.org/docs/changelog>
- Versions 3.2.6 (released 2020-06-10) and before
<https://archivedocs.graylog.org/en/3.2/pages/enterprise/changelog.html>

We appreciate your loyalty to the Graylog Open Community,

David Sciuto
Senior Principal Community Manager