End of Life - Hash Checking in Malware Scan via Third Party Database

Bulletin Date: September 27, 2023

Tenable currently provides the ability for malware hash checking against a third party database from ReversingLabs. As of April 30, 2024, this functionality will no longer be available. See link for more information.

Customers will receive continued support through the Last Date of Support. Table 1 describes the end of life milestones and definitions for the impacted products(s).

Table 1. End of Life Milestones and Dates for Hash Checking in Malware Scan via Third Party Database

Milestone	Definition	Date
End of Life (EoL) Announcement Date	Announcement of the date at which the end of life of a product will be distributed publicly.	September 27, 2023
End of Life Last Date of Support	The last date to receive product support. After this date, support is no longer available and the product is considered obsolete.	April 30, 2024

Product Migration Notes:

Customers can continue to upload their own set of malicious hashes against which the processes and files on the system being scanned will be checked. This feature and behavior would remain unchanged. More information on setting up such scans is available here.

If customers are using the ReversingLabs malware hash checking and the end of support date noted here has been reached, they can harden their security posture and restrict outbound connections to *.l2.nessus.org and can leverage the Disable DNS Resolution setting in products. These two requirements were specific to the ReversingLabs integration and are no longer needed.

FAQs:

- To which products does this apply?
  - Tenable Nessus
  - Tenable Vulnerability Management
  - Tenable Security Center
  - Tenable Container Security
- Which plugins are affected by this change?

  These plugins would stop reporting malicious hashes from our service using the ReversingLabs integration:

  - 59275 Malicious Process Detection
  - 88961 Malicious File Detection

Tenable Technical Support

Technical Support is available to ensure your technical issues or usage questions are resolved in a timely manner. Tenable Support experts are available 24 hours a day, 7 days a week, and are available via a variety of convenient methods, including the Tenable Community, phone, and chat.

Customers with Tenable Technical Support are entitled to a number of predetermined technical support contacts who may: create cases, search the knowledge base, review product documentation, and download software updates. For more details, please refer to the Tenable Technical Support Guide.

Tenable Professional Services

Tenable offers a wide range of services programs to maximize the impact of your investment. With professional services from Tenable and our certified partners, you can reduce your IT risk quickly and achieve rapid time to value. From advisory workshops and quick deployment options to periodic health checks and custom services, we enable you to realize the full potential of your investment. Our team goes beyond basic installation services to partner with you, ensuring your success before, during and after deployment. For more information about Tenable Professional Services, refer to: https://www.tenable.com/services.

For More Information

For more information about the Tenable product offering, please visit the following pages:
Tenable Attack Surface Management: https://www.tenable.com/products/tenable-asm
Tenable Cloud Security: https://www.tenable.com/products/tenable-cs
Tenable One: https://www.tenable.com/products/tenable-one
Tenable Vulnerability Management: https://www.tenable.com/products/tenable-io
Tenable Lumin: https://www.tenable.com/products/tenable-lumin
Tenable Nessus: https://www.tenable.com/products/nessus
Tenable Security Center: https://www.tenable.com/products/tenable-sc
Tenable Identity Exposure: https://www.tenable.com/products/tenable-ad
Tenable OT Security: https://www.tenable.com/products/tenable-ot
Tenable Core: https://docs.tenable.com/Core.htm

v.1.0a