POLICY DOCUMENT: SECURITY VALIDATION SOFTWARE VERSION SUPPORT

This message communicates important information for customers on how the Mandiant Security Validation team supports releases of software over the lifecycle of the product.

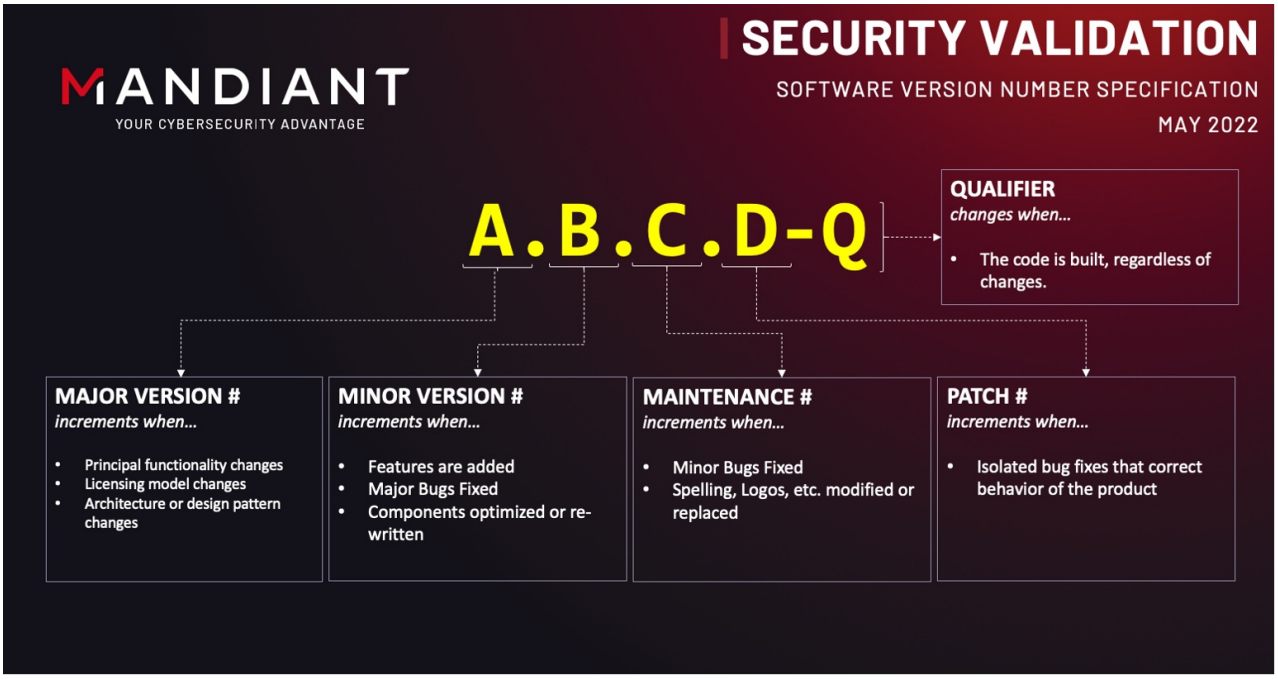
To prioritize uptime and reduce the risk of any unanticipated issues, Mandiant recommends the following:

- Organizations are strongly encouraged to upgrade to the latest version of released software whenever possible.
- Organizations are strongly encouraged to first deploy new versions of software within a representative lab or staging environment.

As new versions of the software are released, Mandiant will always support current versions. However, organizations that elect not to upgrade should understand support for older versions of software will cease when a release is more than 2 “minor” versions behind current. Further, Mandiant is unable to support content related issues found on end-of-life Directors requiring an upgrade. In most cases, this will result in organizations needing to upgrade to a supported version and reproduce the issue before a support ticket can be addressed.

After a new version of content is released, Mandiant will always support the most recent version of published content. However, organizations need to understand Security Validation Content requires a minimum version of software. Organizations should not expect content updates will import or run on unsupported software versions. In most cases, organizations will need to upgrade to the latest compatible content pack and reproduce the issue before a support ticket can be addressed.

For reference, the release version number format is defined as follows:



Supported Versions

Version	Release Date	Status
4.14.6.1	2026-05-19	Supported
4.14.6.0	2026-05-12	Supported
4.14.5.0	2026-02-19	Supported
4.14.4.1	2025-10-30	Supported
4.14.4.0	2025-09-04	Supported
4.14.3.4	2025-08-14	Supported
4.14.3.3	2025-07-17	Supported
4.14.3.2	2025-06-24	Supported
4.14.3.1	2025-05-08	Supported
4.14.3.0	2025-03-25	Supported
4.14.2.3	2025-02-06	Supported
4.14.2.0	2024-11-21	Supported
4.14.1.1	2024-11-04	Supported
4.14.1.0	2024-08-15	Supported
4.14.0.2	2024-05-16	Supported
4.14.0.1	2024-05-07	Supported
4.14.0.0	2024-04-15	Supported
4.13.0.0	2024-02-26	Supported
4.12.4.1	2024-01-23	Limited
4.12.4.0	2023-12-12	Limited
4.12.3.0	2023-11-21	Limited
4.12.2.0	2023-11-09	Limited
4.12.1.0	2023-10-27	Limited
4.12.0.1	2023-11-09	Limited
4.12.0.0	2023-09-29	Limited
4.11.3.0	2023-09-12	EoSL
4.11.2.0	2023-08-17	EoSL
4.11.1.0	2023-07-31	EoSL

Version	Release Date	Status
4.11.0.0	2023-06-20	EoSL
4.10.5.0	2023-06-07	EoSL
4.10.4.0	2023-05-25	EoSL
4.10.3.0	2023-05-18	EoSL
4.10.2.3	2023-05-10	EoSL
4.10.2.2	2023-04-26	EoSL
4.10.2.1	2023-04-12	EoSL
4.10.2.0	2023-03-13	EoSL
4.10.1.0	2023-02-13	EoSL
4.10.0.1	2023-01-30	EoSL
4.10.0.0	2023-01-12	EoSL
4.9.1.2	2022-11-14	EoSL
4.9.1.1	2022-10-31	EoSL
4.9.1.0*	2022-10-19	EoSL
4.9.0.1*	2022-09-26	EoSL
4.9.0.0*	2022-09-22	EoSL
4.8.4.3	2022-11-03	EoSL
4.8.4.2	2022-09-12	EoSL
4.8.4.1	2022-07-28	EoSL
4.8.4.0	2022-07-12	EoSL
4.8.3.1	2022-05-24	EoSL
4.8.3.0	2022-04-26	EoSL
4.8.2.0	2022-03-21	EoSL
4.8.1.0	2022-02-08	EoSL
4.7.0.0	2021-12-15	EoSL
4.6.3.0	2021-12-17	EoSL
4.6.2.0	2021-11-29	EoSL
4.6.1.0	2021-10-06	EoSL

Limited Support means there is support only for CRITICAL level fixes on an as-needed basis.

* The network map may appear with a "license expired" watermark. This can be mitigated by upgrading to a subsequent supported release.

Example

Using the release of version 4.12.0.0 as an example, software release versions up to the most recent 4.10.x.x would be supported for critical fixes on an as-needed basis only. As the best practice suggests, organizations should be current to at least the latest minor release. In this example, 4.10.0.0 serves as the last supported release. Releases flagged as EoSL have reached the end of their service life and are no longer supported.