Scheer PAS Release Management

Versioning

The PAS version is defined as follows:

- · year.release.patch
- Example: 22.1.2

| Version Definitions | | |
|---------------------|---|--|
| Release | A release contains new components, new features and/or improvements. When upgrading to a new release, a manual migration of existing models or services might be necessary by the customer. | |
| Patch | A patch contains only bug and security fixes. | |

On this Page:

- Versioning Release Frequency
- Maintenance
 - Classification Schemes
 - Bug Severity
 - Security Severity

Release Frequency

Releases will be announced at least one month before release date. The following release cycle is aimed for:

- 4 releases per year (one of them as LTS release)
- patches according to maintenance

Maintenance

Maintenance will be delivered for the following releases:

| Release | Maintenance Schedule | Maintenance Details |
|---------------------------------------|---|---|
| Latest release | The latest release will be under maintenance until the next release. | patches for security issuesbug fixes |
| LTS release (Long Term Support) | An LTS release will be under maintenance for 1 year after its release date. | patches for security issuesbug fixes |

Patch releases will be delivered only for major and critical bugs as well as for high and critical security vulnerabilities, according to the following classification schemes.

Bugs which are classified as trivial or minor, and security vulnerabilities classified as low or medium will be fixed with the next release.

Classification Schemes

Bug Severity

| Bug Severity | Description |
|-----------------|--|
| Trivial | The defect does not affect functionality. A workaround is not required. The defect does not affect productivity or efficiency. Includes UI issues. |
| Minor | The defect either affects minor functionality or it affects major functionality but can be easily worked around. |
| Major | The defect affects major functionality. Either there is no workaround or an existing workaround significantly affects productivity and efficiency. |
| Critical | The defect affects the availability or business-critical functionality of production systems. Urgent business-critical work cannot be carried out. There is no workaround. |

Security Severity

The severity of security vulnerabilities is classified according to the Common Vulnerability Scoring System (CVSS) for potential vulnerabilities in internal as well as third-party components.



For detailed information see National Institute of Standards and Technology (U.S.).

| Vulnerability Severity | CVSS Score Range |
|------------------------|------------------|
| None | 0.0 |
| Low | 0.1 - 3.9 |
| Medium | 4.0 - 6.9 |
| High | 7.0 - 8.9 |
| Critical | 9.0 - 10.0 |