

Security Policy

Vulnerability and patch management

Information security

|  |  |
| --- | --- |
|  |  |
| Vulnerability and patch management |  |
| Number | [Number] |
| Issued on | 30.06.2022 |
| Through | Chief Information Security Officer |
| Entry into force | 30.06.2022 |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH |
| Topic | Compliance |
| Responsible function | Information security |
| Responsible person | Dirk Franken |
| Overriding regulation | SÜDVERS Information Security Policy |
| Replaces | n/a |
| Applicable documents |  |
| Validity | Until further notice |
| Last | 14.07.2025 |
| Next review | 07.01.2026 |
| Publication | SÜDVERS Intranet |
| Classification | Internal |
| Archive | Document management system |
| Organizational system | [Organizational system] |
| Languages |  |
| Formats |  |
| Remarks |  |

Table of contents

[1 Principles 4](#_Toc107558322)

[2 Goals 4](#_Toc107558323)

[3 Controls 4](#_Toc107558324)

[3.1 Check for weak points 5](#_Toc107558325)

[3.2 Patch management 6](#_Toc107558326)

[3.2.1 Emergency fixes 7](#_Toc107558327)

# Principles

Vulnerabilities in IT systems need to be identified and remedied in a structured and efficient way, and the relevant controls in the environment need to be assessed.

# Goals

In order to protect SÜDVERS, the degree of vulnerability of IT systems must be assessed for each threat event and appropriate measures taken.

# Controls

Standards/procedures for the management and operation of IT systems must be supported by a system and software vulnerability management process to identify (not limited to) system and software vulnerabilities:

* Business applications, operating system software and firmware (e.g. on servers, mobile devices)
* Computer equipment (including servers, desktop computers, laptops, tablets, smartphones...)
* Virtual systems (e.g. virtual servers and virtual desktops)
* Network storage systems (including Storage Area Network (SAN) and Network-Attached Storage (NAS))
* Network equipment (such as routers, switches, gateways, network IDS/IPS devices, wireless access points and firewalls)
* VoIP telephony software and telephony/video conferencing devices
* SmartTVs
* Office equipment (e.g. network printers, photocopiers, fax machines, scanners and multifunctional devices (MFDs))
* CCTV cameras
* Embedded systems

to recognize and treat.

The process for managing system and software vulnerabilities must:

* be documented
* be approved by the process owner within IT
* be supported by related IT teams with defined roles and responsibilities for vulnerability management
* ensure that operational responsibility for the respective system environments is assigned
* be used continuously (e.g. at least daily).

The process for managing system and software vulnerabilities must serve this purpose:

* detect system and software vulnerabilities as soon as they become known (e.g. by tracking CERT reports or subscribing to vulnerability notification services)
* Identify and procure necessary patches as soon as they are available to fix discovered vulnerabilities
* decide when to install patches (e.g. by determining whether the vulnerabilities are already being actively used, by assessing the potential impact on SÜDVERS after deployment, by determining the criticality of patches (using the Common Vulnerability Scoring System (CVSS), the vendor's criticality rating of patches, the Common Configuration Enumeration Project or similar methods)
* ensure the documentation of the applied patches (e.g. with the help of an inventory register, a configuration management database (CMDB) or similar).

## Check for weak points

The system and software vulnerability management process must be supported by performing vulnerability scans of business applications, IT systems and network devices to

* Identify system and software vulnerabilities in business applications, IT systems and network devices
* determine the extent to which business applications, IT systems and network devices are exposed to threats
* identify what could be affected by certain vulnerabilities
* Set priorities for the elimination of weaknesses

Vulnerability scans of business applications, IT systems and network devices must:

* using automated vulnerability scanning software or a commercial vulnerability scanning service
* regularly, whereby the minimum inspection intervals are defined as follows:
  + for systems that are accessible from untrusted systems via untrusted networks (such as the Internet): daily
  + for systems not covered by the above point: weekly

be carried out.

The implementation of the vulnerability check must:

* be restricted to a limited number of authorized persons
* be carried out using approved and specific systems

## Patch management

System and software vulnerabilities must be remedied with the help of a patch management process that:

* Defines methods for validating patches (e.g. ensuring that the patch comes from an authorized source)
* for patches that affect application logic, assesses the business impact of implementing patches (or not implementing a particular patch)
* describes methods for timely deployment (installation) of patches (e.g. grouping of multiple patches and use of software distribution tools)
* Describes methods for providing patches for systems that are only rarely connected to the network (e.g. employees traveling)
* describes methods for dealing with the failed installation of a patch (e.g. reinstalling the patch)
* ensures that appropriate alternative protective measures are taken if a patch or workaround to fix a vulnerability is not available or the patch would have a significant negative impact on the functionality of the overall system.[[1]](#footnote-1)
* ensures that status information regarding the patch status of the SÜDVERS IT systems can be created.

For the provision of patches to fix vulnerabilities with a CVSS score between 4.0 and 10.0 or for the propagation of attacks without user intervention, the following maximum time limits apply:

* for systems that are accessible from untrusted systems via untrusted networks (such as the Internet):
  + if the CVSS score is between 7.0 and 10.0
    - within 1 day after release of the patch
  + if the CVSS score is between 4.0 and 6.9
    - within 1 week of the patch being released,
* for systems that are accessible from untrusted systems via untrusted networks (such as the Internet) or that are located in internal network segments and are accessed from systems in external DMZs:
  + if the CVSS score is between 9.0 and 10.0
    - within 1 day after release of the patch
  + if the CVSS score between 4.0 and 8.9
    - within 1 week of the patch being released,
    - if the individual system is fully protected by network or host-based IPS covering the vulnerability, within 2 weeks
* for internal systems (not covered by the above points):
  + within 1 week after the release of the patch
  + within 2 weeks if the individual system is fully protected by network-based IPS or host-based IPS covering the vulnerability

The maximum time frame for the provision of patches with a CVSS score lower than 4.0 is set as follows

* within 1 month after release of the patch
* within 3 months if the individual system is fully protected by network-based IPS or host-based IPS covering the vulnerability

### Emergency fixes

In the event that systems are vulnerable to attacks for which no released patch is available, additional checks must be carried out as described below.

Documented standard operating procedures for the application of emergency fixes must be defined and documented in order to be able to react promptly and safely to emergencies and at the same time reduce interruptions for SÜDVERS.

Emergency fixes must be subject to the standard disciplines of change management

Any emergency corrections applied must be documented.

Once an emergency has ended, the authorization for emergency access must be revoked immediately on the recommendation of the manufacturers concerned.

Any emergency corrections applied must be reviewed regularly to ensure that they do not remain in force permanently.

1. For systems that are no longer supported by the manufacturers, this can be achieved by using host-based IPS systems (so-called virtual patching), by including services and software in a whitelist or by restricting system functionality (reduced services, fewer access rights to other systems, increased monitoring in conjunction with the placement of the corresponding systems in specially secured network segments). [↑](#footnote-ref-1)