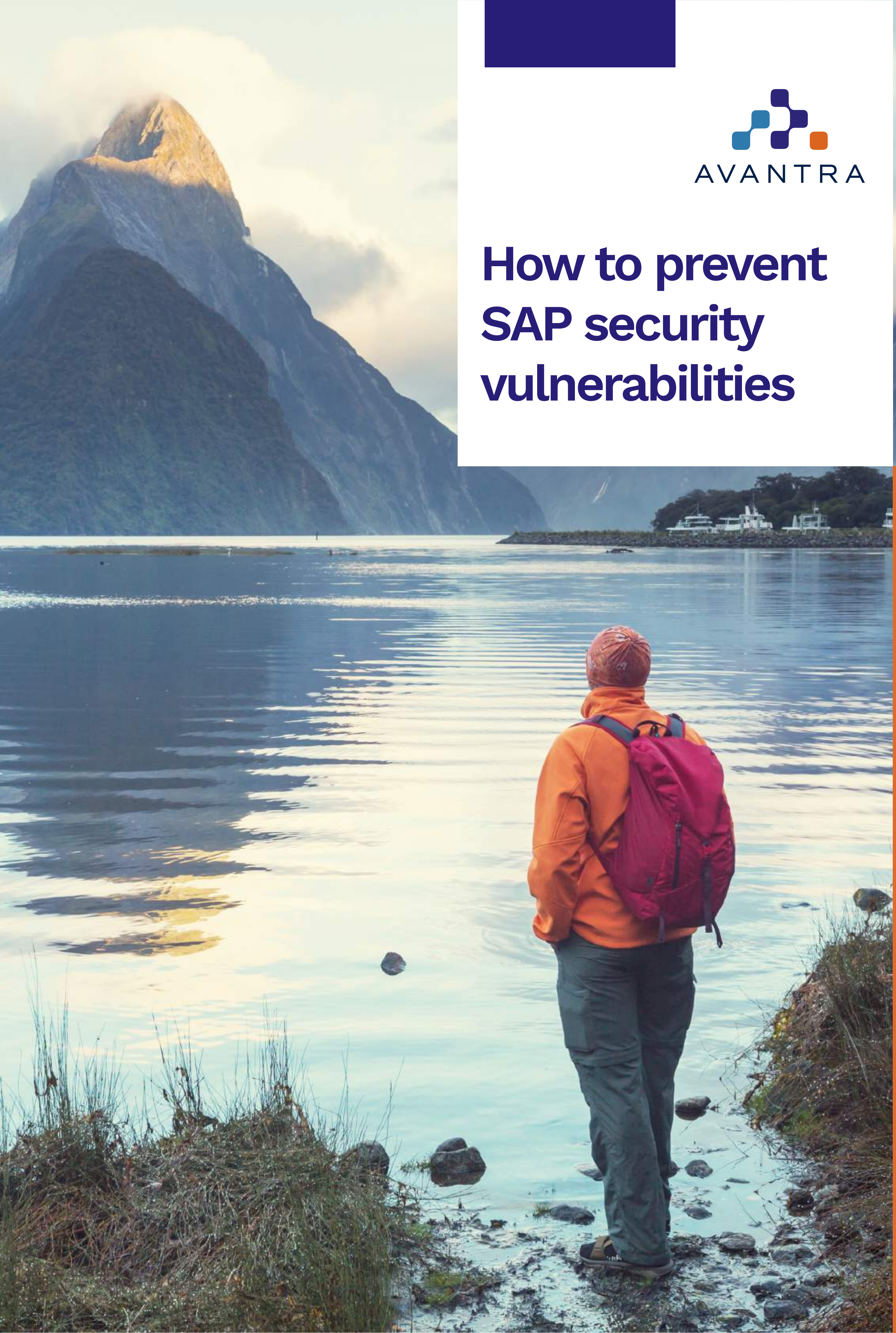
AVANTRA

How to prevent SAP security vulnerabilities



About the author

Tyler Constable is a senior SAP professional who's been managing, deploying and monitoring ERP systems for over 15 years. He co-hosts the popular "What's SAPpening" podcast and is a prominent presenter of the Mastering Avantra training programme. Tyler is passionate about IT operations security and automation, and is an active member of the SAP community.

Tyler leads Avantra's sales engineering and works with SAP teams in enterprises and service providers all over the world. He holds a BSc in Information Science and Technology (IST) from the University of Wisconsin-Milwaukee.

Tyler Constable,
Directer of Sales Engineering

Introduction

SAP creates some of the world's most popular products for managing information, with more than 400 million users worldwide. But SAP connectivity presents one of the biggest security risks for your company.

In this ebook, we'll discuss the steps you can take to secure your SAP systems. We'll also explore ways in which SAP systems can be compromised, as well as some of the ways to prevent this from happening.

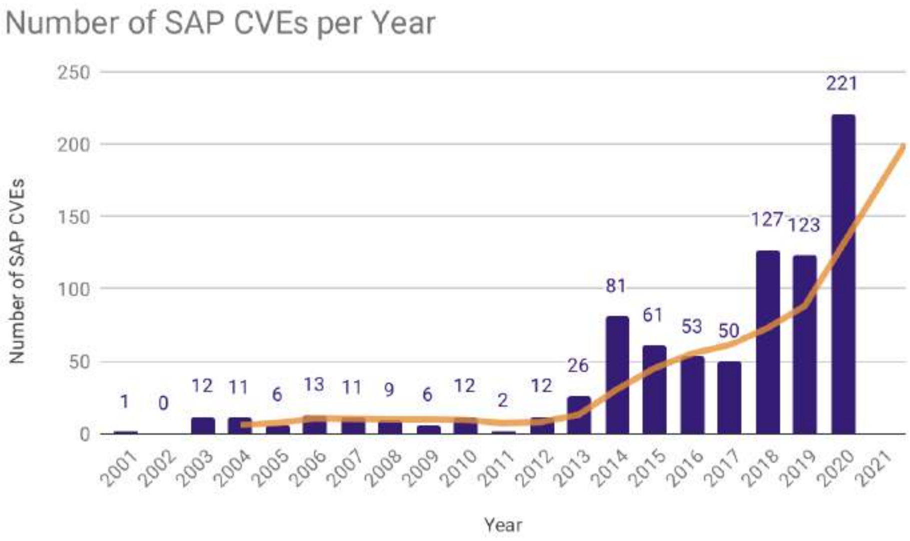
Why should I care?

If you have read the headline, your first response probably was along the lines of "this should be a topic of a training course for people developing SAP applications". And yes, we all like the vulnerabilities most that are detected during software development and testing before the rubber hits the floor. However, does a vulnerability exist only because it's in the code, or does it come to life only once the software is running in a particular environment?

Whatever the answer, it's your business at risk. And even if you cannot fix a bug in SAP NetWeaver yourself, there is a lot you can do to mitigate this risk. And hence to prevent SAP security vulnerabilities to be exploited.

If you're following the news around SAP security, you might ask: is this just hype because of the one rather prominent incident discovered in 2020 by Onapsis Research Labs? The infamous CVE-2020-6287, better known as SAP RECON vulnerability (Remotely Exploitable Code On NetWeaver), marks the first one with a CVSS score of 10, but it's by far not the only vulnerability, and not even the only one with a high exploitability score. If you need a quick recap, check out our blog on CVSS & SAP System Vulnerability.

If you look at the Common Vulnerabilities and Exposures (CVE) for SAP over the last twenty years, the picture looks like this:



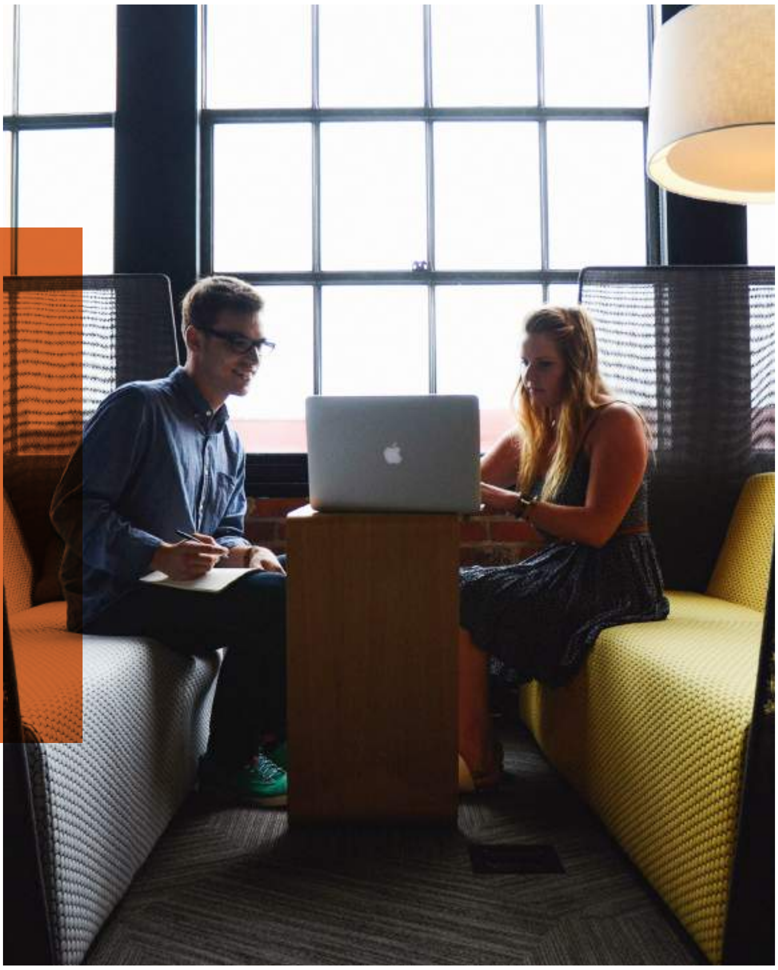
The data is retrieved from the CVE Details website, and we added a little trend line. Of course, there is a huge difference between the severities of these vulnerabilities. They range from small impact (e.g. no or only a small amount of sensitive data involved) to high impact combined with a low attack complexity. But there is a clear upward trend. It's not a question if the next RECON will happen, but only when it will happen.

A chain is no stronger than its weakest link

Even after 20 years in this business I still get the impression SAP landscapes, or even the whole SAP ecosystem, is a world of its own. When it comes to security, worlds of their own tend to not do well. Enterprise security is only as strong as its weakest link, however, this implies it has to be linked in the first place. So it’s not only the CIO who has to get off their ERP island, security does as well.

> **Unsecure network access allows connectivity from untrusted sources in the first place, with the potential to let an unauthenticated attacker access sensitive data.**

Whenever I read about the possible impact of a critical vulnerability I wonder how many NetWeaver application servers apparently allow network access from the Internet. Let’s hope at least it’s not the SAP Solution Manager being exposed this way. Unsecure network access allows connectivity from untrusted sources in the first place, with the potential to let an unauthenticated attacker access sensitive data. There may be use cases, but the figures let me assume in some companies SAP security is not well integrated into the enterprise security strategy.



Avantra helps you to keep systems locked down and provides peace of mind by knowing your SAP systems are secure.

SAP security and peace of mind

The good news is that starting with S/4HANA, security by default arrives in SAP landscapes. For all older systems, hardening is the first step to improve your security in all areas, where the secure variant is not the default. But system hardening can go much further than that: if your business operates in regulated environments such as GxP or SOX, there is far more you need to consider to meet these standards.

Fortunately, this is an area where Avantra can be of great help. You can define the security policies for your profiles while Avantra verifies they are all matched. And starting this fall, you can even initiate to automatically adjust profile parameters if they deviate from your policies - without user interaction.

SAP HotNews and SAP Security Notes

When it comes to vulnerability management or patch management, the SAP Security Notes and SAP HotNews are home base for SAP customers. They are also part of the SAP Product Security Response Space where SAP outlines their responses to CVEs. If you do not want to rely purely on the responses from SAP, you can query the CVE Details for vendor SAP, or for instance use this RSS feed link. SAP HotNews includes all SAP Security Notes with a CVSS score of 9 or higher.

The difficult bit is always to verify where the fixes outlined in the SAP Notes need to be applied. Some SAP systems might not be affected at all, some may have the SAP Note applied already. Of course, this task is the more difficult the more complex your landscape is.

But there is some exciting news for you:

Starting this Fall, Avantra will automatically determine the SAP HotNews available and compare these with the Notes already implemented on each managed SAP system. It will automatically suggest implementing the missing ones on a per-system basis.

Auditing and change management

Another important pillar in your enterprise cybersecurity strategy is to verify security controls are properly implemented. Or in simpler terms: periodic security audits. The underpinning idea of a security strategy is the detection and assessment of risks, and putting controls in place to mitigate these risks. This is usually done by policies that prescribe said controls. The purpose of an audit in essence is to verify the policies are in place and to review evidence proving the policies are followed. And there is no exception for SAP applications.

An essential part, if not the most important one, is to track changes. The single most common root cause for security incidents is human error. As long as it is us humans who perform system changes, planning, tracking, approving, and reviewing these changes are of utmost importance to avoid failure.

The built-in reporting functions tremendously simplify to display all changes over a period of time. And back in those days when Avantra was an MSP, we were able to provide evidence during security audits more or less only by generating Service Level Reports.

At Avantra we track and record changes to SAP systems and databases automatically, even if they have not been planned and approved.

Monitoring

All security measures, as well as the most important potential threats, should be permanently monitored. So, a reliable and robust monitoring solution is at the very heart of every security strategy in all organizations. However, there is a trend to be seen in recent years where monitoring more and more shifts to primarily looking into application performance.

When it comes to security, application performance monitoring will probably not help you a great deal. Questions like: are standard passwords configured for system users, are system changes prevented in productive ABAP clients, is the audit log configured properly, are certificates about to expire - they will only be answered by a solution tailored to support SAP operations, like Avantra.

And while these checks cannot prevent vulnerabilities that most likely exist somewhere deep down in the code, they can potentially help you to prevent these vulnerabilities from being exploited, or at least limit their impact.

Learn more about Avantra today www.avantra.com

AVANTRA

IT Operations, Automated.

UK Headquarters
Parkshot House
5 Kew Road
Richmond TW9 2PR
United Kingdom

Switzerland
Lautengartenstr. 6
4052 Basel
Switzerland

North America
33 West Monroe Street
Suite 1025
Chicago Illinois 60603
United States

Document Version:
2021-06

This preliminary information is subject to change without notice and is provided “as is” with no warranty. Syslink Xandria Ltd and its subsidiaries shall not be liable for any direct, indirect, special, incidental or consequential damages in connection with the use of this material. This material is not intended to be a binding agreement.