SSA-661247: Apache Log4j Vulnerabilities (Log4Shell, CVE-2021-44228, CVE-2021-45046) - Impact to Siemens Products

Publication Date: 2021-12-13
Last Update: 2022-01-05
Current Version: V2.2
CVSS v3.1 Base Score: 10.0

SUMMARY

On 2021-12-09, a vulnerability in Apache Log4j (a logging tool used in many Java-based applications) was disclosed, that could allow remote unauthenticated attackers to execute code on vulnerable systems. The vulnerability is tracked as CVE-2021-44228 and is also known as “Log4Shell”.

On 2021-12-14 an additional denial of service vulnerability (CVE-2021-45046) was published rendering the initial mitigations and fix in version 2.15.0 as incomplete under certain non-default configurations. Log4j versions 2.16.0 and 2.12.2 are supposed to fix both vulnerabilities.

On 2021-12-17, CVE-2021-45046 was reclassified with an increased CVSS base score (from 3.7 to 9.0). The potential impact of CVE-2021-45046 now includes - besides denial of service - also information disclosure and local (and potential remote) code execution.

Siemens is currently investigating to determine which products are affected and is continuously updating this advisory as more information becomes available. See section Additional Information for more details regarding the investigation status.

Note: two additional vulnerabilities were published for Apache Log4j, the impact of which are documented in SSA-501673: https://cert-portal.siemens.com/productcert/pdf/ssa-501673.pdf (CVE-2021-45105) and SSA-784507: https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf (CVE-2021-44832).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Advantage Navigator Energy & Sustainability: All versions < 2021-12-13	Vulnerability CVE-2021-44228 fixed on central cloud service starting 2021-12-13; no user actions necessary See further recommendations from section Workarounds and Mitigations
Advantage Navigator Software Proxy V6: All versions < V6.3	Update to V6.3 or later version See further recommendations from section Workarounds and Mitigations
Building Operator Discovery Distribution for the Connect X200 Gateway: All versions < V3.0.30	Update to V3.0.30 or later version https://support.industry.siemens.com/cs/ww/en/view/109805593/ See further recommendations from section Workarounds and Mitigations
Building Operator Discovery Distribution for the Connect X300 Gateway: All versions < V3.0.29	Update to V3.0.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109805593/ See further recommendations from section Workarounds and Mitigations

Building Twin - 360° Viewer: All versions	Vulnerability CVE-2021-44228 fixed on central cloud service; no user actions necessary See further recommendations from section Workarounds and Mitigations
Capital: All versions >= 2019.1 SP1912 only if Teamcenter integration feature is used	Currently no remediation is available Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/MG618363 See further recommendations from section Workarounds and Mitigations
Cerberus DMS: V5.0, V5.1 with Advanced Reporting EM installed	Remove the JndiLookup class from the class-path. Detailed instructions are available at https://support.industry.siemens.com/cs/ww/en/view/109805562/ See further recommendations from section Workarounds and Mitigations
Comos Desktop App: All versions	Currently no remediation is available Uninstall “Teamcenter Client Communication System (TCSS)” or block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
Desigo CC: V3.0, V4.0, V4.1, V4.2 with Advanced Reporting EM installed	Remove the JndiLookup class from the class-path. Detailed instructions are available at https://support.industry.siemens.com/cs/ww/en/view/109805562/ See further recommendations from section Workarounds and Mitigations
Desigo CC: V5.0, V5.1 with Advanced Reporting or Info Center EM installed	Remove the JndiLookup class from the class-path. Detailed instructions are available at https://support.industry.siemens.com/cs/ww/en/view/109805562/ See further recommendations from section Workarounds and Mitigations
E-Car OC Cloud Application: All versions < 2021-12-13	Vulnerability CVE-2021-44228 fixed on central cloud service starting 2021-12-13; no user actions necessary See further recommendations from section Workarounds and Mitigations
Energy Engage: V3.1	Find detailed remediation and mitigation information on the EnergyIP docs portal at: https://docs.emeter.com/display/public/WELCOME/EnergyIP+Security+Advisory+for+Log4Shell+Vulnerability See further recommendations from section Workarounds and Mitigations

EnergyIP: V8.5, V8.6, V8.7, V9.0	Find detailed remediation and mitigation information on the EnergyIP docs portal at: https://docs.emeter.com/display/public/WELCOME/EnergyIP+Security+Advisory+for+Log4Shell+Vulnerability Note: EnergyIP V8.5 and V8.6 applications are not directly affected, but CAS is. See further recommendations from section Workarounds and Mitigations
EnergyIP Prepay V3.7: All versions only affected by CVE-2021-44228	Currently no remediation is available Set the parameter log4j2.formatMsgNoLookups to 'true' Only installations with POS/IOSaccess component are affected See further recommendations from section Workarounds and Mitigations
EnergyIP Prepay V3.8: All versions < V3.8.0.12 only affected by CVE-2021-44228	Update to V3.8.0.12 or later version See further recommendations from section Workarounds and Mitigations
Enlighted Amaze: All versions < 2021-12-10	Vulnerabilities fixed on central cloud services starting 2021-12-10; no user actions necessary For Comfy and Enlighted, see also chapter Additional Information below See further recommendations from section Workarounds and Mitigations
Enlighted Where: All versions < 2021-12-11	Vulnerabilities fixed on central cloud services starting 2021-12-11; no user actions necessary For Comfy and Enlighted, see also chapter Additional Information below See further recommendations from section Workarounds and Mitigations
Geolus Shape Search V10: All versions >= V10.2	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8601468 See further recommendations from section Workarounds and Mitigations
Geolus Shape Search V11: All versions	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8601468 See further recommendations from section Workarounds and Mitigations

GMA-Manager: All versions >= V8.6.2j.398 and < V8.6.2.472	Update to V8.6.2.472 or later version https://support.industry.siemens.com/cs/ww/en/view/109805665/ See further recommendations from section Workarounds and Mitigations
HEEDS Connect: All versions	HEEDS Connect team will contact all impacted customers to deploy a new log4j version. This action will secure your installation against Log4Shell vulnerability. For further information see: https://support.sw.siemens.com/en-US/knowledge-base/PL8601661 See further recommendations from section Workarounds and Mitigations
HES UDIS: All versions	Currently no remediation is available Specific mitigation information has been released for the local project teams with the request of immediate deployment. A patch is planned for the next regular release. See further recommendations from section Workarounds and Mitigations
Industrial Edge Management App (IEM-App): All versions	Exposure to vulnerability is limited as IEM-App runs in IEM-OS and IEM-OS is not intended to be exposed to public internet and should be operated in a protected environment. Please refer to the Industrial Edge - Security overview https://support.industry.siemens.com/cs/ww/en/view/109804061 See further recommendations from section Workarounds and Mitigations
Industrial Edge Management Hub: All versions < 2021-12-13	Vulnerabilities fixed on central cloud service starting 2021-12-13; no user actions necessary See further recommendations from section Workarounds and Mitigations
Industrial Edge Management OS (IEM-OS): All versions	Exposure to vulnerability is limited as IEM-OS is not intended to be exposed to public internet and should be operated in a protected environment. Please refer to the Industrial Edge - Security overview: https://support.industry.siemens.com/cs/ww/en/view/109804061 - For more information, see https://support.industry.siemens.com/cs/ww/en/view/109805619 See further recommendations from section Workarounds and Mitigations
jROS for Spectrum Power 4: V4.70 SP9	Currently no remediation is available Apply the mitigation measures provided via customer support See further recommendations from section Workarounds and Mitigations
jROS for Spectrum Power 7: V21Q4	Currently no remediation is available Apply the mitigation measures provided via customer support See further recommendations from section Workarounds and Mitigations

Mendix Applications: All versions	Although the Mendix runtime itself is not vulnerable to this exploit, we nevertheless recommend to upgrade log4j-core to the latest available version if log4j-core is part of your project. This advice is regardless of the JRE/JDK version the app runs on. https://status.mendix.com/incidents/8j5043my610c See further recommendations from section Workarounds and Mitigations
MindSphere App Management Cockpits (Developer& Operator): All versions < 2021-12-16	Vulnerabilities fixed with update on 2021-12-16; no user actions necessary See further recommendations from section Workarounds and Mitigations
MindSphere Asset Manager: All versions < 2021-12-16	Vulnerabilities fixed with update on 2021-12-16; no user actions necessary See further recommendations from section Workarounds and Mitigations
Mindsphere Cloud Foundry: All versions < 2021-12-14	Although the Cloud Foundry environment itself is not vulnerable to this exploit, we nevertheless recommend to upgrade log4j-core to the latest available version if log4j-core is part of your project. https://support.sw.siemens.com/en-US/product/268530510/knowledge-base/PL8600797 See further recommendations from section Workarounds and Mitigations
Mindsphere Cloud Platform: All versions < 2021-12-11	Vulnerabilities fixed on central cloud service starting 2021-12-11; no user actions necessary See further recommendations from section Workarounds and Mitigations
MindSphere IAM (User Management/ Settings): All versions	Vulnerabilities fixed with update on 2021-12-16; no user actions necessary See further recommendations from section Workarounds and Mitigations
MindSphere Integrated Data Lake: All versions < 2021-12-16	Vulnerabilities fixed with update on 2021-12-16; no user actions necessary See further recommendations from section Workarounds and Mitigations
MindSphere Notification Service: All versions < 2021-12-16	Vulnerabilities fixed with update on 2021-12-16; no user actions necessary See further recommendations from section Workarounds and Mitigations
MindSphere Predictive Learning: All versions	Vulnerabilities fixed with update on 2021-12-23; no user actions necessary See further recommendations from section Workarounds and Mitigations
MindSphere Usage Transparency Service: All versions < 2021-12-16	Vulnerabilities fixed with update on 2021-12-16; no user actions necessary See further recommendations from section Workarounds and Mitigations

MindSphere Visual Explorer: All versions	Vulnerabilities fixed with update on 2021-12-21; no user actions necessary See further recommendations from section Workarounds and Mitigations
NX: All versions	Currently no remediation is available Find detailed mitigation steps at: https://solutions.industrysoftware.automation.siemens.com/view.php?si=sfb-nx-8600959 See further recommendations from section Workarounds and Mitigations
NXpower Monitor: All versions < 2021-12-19	Vulnerabilities fixed on central cloud service starting 2021-12-19; no user actions necessary See further recommendations from section Workarounds and Mitigations
Opcenter EX CP Process Automation Control: All versions >= V17.2.3 and < V18.1	Update to V18.1 or later version to fix CVE-2021-44228 See further recommendations from section Workarounds and Mitigations
Opcenter Intelligence: All versions >= 3.2 only OEM version that ships Tableau	Currently no remediation is available See recommendations from section Workarounds and Mitigations
Operation Scheduler: All versions >= V1.1.3	Update the UAA component to V75.8.3 https://support.industry.siemens.com/cs/ww/en/view/109805673/ See further recommendations from section Workarounds and Mitigations
SENTRON powermanager V4: V4.1, V4.2	Remove the JndiLookup class from the classpath. Detailed instructions are available at https://support.industry.siemens.com/cs/ww/en/view/109805602/ See further recommendations from section Workarounds and Mitigations
SIGUARD DSA: All versions >= 4.2 and < 4.4.1	Update to V4.4.1 or later version See further recommendations from section Workarounds and Mitigations
SIMATIC IPC647D: All versions with affected Adaptec RAID	Check the original vendor advisory of the affected RAID controller configuration software at: https://ask.adaptec.com/app/answers/detail/a_id/17523/~/storage-management-response-to-apache-log4j-remote-code-execution-vulnerability Stop and disable autostart for maxView Storage Manager WebServer. Note: This software is not required for the underlying RAID to work Disable ports 8080/tcp and 8443/tcp in the firewall configuration of the IPC See further recommendations from section Workarounds and Mitigations

SIMATIC IPC647E: All versions with affected Adaptec RAID	Check the original vendor advisory of the affected RAID controller configuration software at: https://ask.adaptec.com/app/answers/detail/a_id/17523/~/storage-management-response-to-apache-log4j-remote-code-execution-vulnerability Stop and disable autostart for maxView Storage Manager WebServer. Note: This software is not required for the underlying RAID to work Disable ports 8080/tcp and 8443/tcp in the firewall configuration of the IPC See further recommendations from section Workarounds and Mitigations
SIMATIC IPC847D: All versions with affected Adaptec RAID	Check the original vendor advisory of the affected RAID controller configuration software at: https://ask.adaptec.com/app/answers/detail/a_id/17523/~/storage-management-response-to-apache-log4j-remote-code-execution-vulnerability Stop and disable autostart for maxView Storage Manager WebServer. Note: This software is not required for the underlying RAID to work Disable ports 8080/tcp and 8443/tcp in the firewall configuration of the IPC See further recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All versions with affected Adaptec RAID	Check the original vendor advisory of the affected RAID controller configuration software at: https://ask.adaptec.com/app/answers/detail/a_id/17523/~/storage-management-response-to-apache-log4j-remote-code-execution-vulnerability Stop and disable autostart for maxView Storage Manager WebServer. Note: This software is not required for the underlying RAID to work Disable ports 8080/tcp and 8443/tcp in the firewall configuration of the IPC See further recommendations from section Workarounds and Mitigations

SIMATIC IPC1047: All versions with affected Adaptec RAID	Check the original vendor advisory of the affected RAID controller configuration software at: https://ask.adaptec.com/app/answers/detail/a_id/17523/~/storage-management-response-to-apache-log4j-remote-code-execution-vulnerability Stop and disable autostart for maxView Storage Manager WebServer. Note: This software is not required for the underlying RAID to work Disable ports 8080/tcp and 8443/tcp in the firewall configuration of the IPC See further recommendations from section Workarounds and Mitigations
SIMATIC IPC1047E: All versions with affected Adaptec RAID	Check the original vendor advisory of the affected RAID controller configuration software at: https://ask.adaptec.com/app/answers/detail/a_id/17523/~/storage-management-response-to-apache-log4j-remote-code-execution-vulnerability Stop and disable autostart for maxView Storage Manager WebServer. Note: This software is not required for the underlying RAID to work Disable ports 8080/tcp and 8443/tcp in the firewall configuration of the IPC See further recommendations from section Workarounds and Mitigations
Simcenter 3D: All versions < 2022.1-2008	Update to 2022.1-2008 or later version https://support.sw.siemens.com/en-US/knowledge-base/PL8603477 Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8601203 See further recommendations from section Workarounds and Mitigations
Simcenter Amesim: All version only if Teamcenter integration feature is used	Currently no remediation is available The workaround is described in this Teamcenter SFB: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further information for Amesim see: https://support.sw.siemens.com/en-US/knowledge-base/PL8601572 See further recommendations from section Workarounds and Mitigations
Simcenter System Architect: All versions only if Teamcenter integration feature is used	Currently no remediation is available The workaround is described in this Teamcenter SFB: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further information for System Architect see: https://support.sw.siemens.com/en-US/knowledge-base/PL8601662 See further recommendations from section Workarounds and Mitigations

Simcenter System Simulation Client for Git: All versions	Currently no remediation is available Find detailed mitigation steps for both server and client installations at: https://support.sw.siemens.com/en-US/knowledge-base/PL8602538 See further recommendations from section Workarounds and Mitigations
Simcenter Testlab: All versions >= 2021.1	Follow the remediation steps documented at: https://support.sw.siemens.com/en-US/knowledge-base/PL8602466 See further recommendations from section Workarounds and Mitigations
Simcenter Testlab Data Management: All versions	Simcenter Testlab Data Management team will contact all impacted customer to deploy the mitigation measures. This action will secure your installation against Log4Shell vulnerability. For further information see: https://support.sw.siemens.com/en-US/knowledge-base/PL8601418 See further recommendations from section Workarounds and Mitigations
SiPass integrated V2.80: All versions	Currently no remediation is available Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
SiPass integrated V2.85: All versions	Currently no remediation is available Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
Siveillance Command: All versions >= V4.16.2.1	Currently no remediation is available Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
Siveillance Control Pro: All versions	Hotfix available for versions >= V2.1 (please contact customer support) Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
Siveillance Identity V1.5: All versions	Update to V1.5 SP4 and apply the patch https://support.industry.siemens.com/cs/ww/en/view/109805657/ See further recommendations from section Workarounds and Mitigations
Siveillance Identity V1.6: All versions	Update to V1.6 SP1 and apply the patch https://support.industry.siemens.com/cs/ww/en/view/109805657/ See further recommendations from section Workarounds and Mitigations

Siveillance Vantage: All versions	Currently no remediation is available Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
Solid Edge CAM Pro: All versions delivered with Solid Edge SE 2020 or later version	Currently no remediation is available See recommendations from section Workarounds and Mitigations
Solid Edge Harness Design: All versions >= 2020 SP2002 only if Teamcenter integration feature is used	Currently no remediation is available Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/MG618363 See further recommendations from section Workarounds and Mitigations
Spectrum Power™ 4: All versions >= V4.70 SP8	Update to V4.70 SP9 and apply the mitigation measures or the patch provided via customer support See further recommendations from section Workarounds and Mitigations
Spectrum Power™ 7: All versions >= V2.30 SP2	Update to V21Q4 and apply the mitigation measures or the patch provided via customer support See further recommendations from section Workarounds and Mitigations
Teamcenter: All versions >= V13.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Active Workspace: All versions >= V4.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Briefcase Browser: All versions >= V13.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations

Teamcenter Data Share Manager: All versions >= V13.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Deployment Center: All versions >= V3.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Dispatcher Service: All versions >= V11.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter EDA: All versions >= V2.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter FMS: All versions >= V11.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Integration for CATIA: All versions < 13.0.1.2	Update to V13.0.1.2 or later version https://support.sw.siemens.com/knowledge-base/PL8602463 See further recommendations from section Workarounds and Mitigations
Teamcenter Integration Framework: All versions <= V13.2	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations

Teamcenter MBSE Gateway: All versions >= V4.0	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Mendix Connector: V1.0	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Microservices Framework: All versions >= V5.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Polarion Integration: All versions >= V5.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Rapid Start: All versions >= V13.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Reporting and Analytics: All versions based on Java SOA client >= V11.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations

Teamcenter Requirements Integrator: All versions based on Java SOA client >= V11.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Retail Footwear and Apparel: All versions >= V4.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Security Services: All versions >= V11.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Supplier Collaboration: All versions >= V5.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter System Modeling Workbench: All versions based on Java SOA client >= V11.3	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Teamcenter Technical Publishing: All versions >= V2.10	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700 See further recommendations from section Workarounds and Mitigations
Tecnomatix eBOP Manager Server: V14.1, V15.0, V15.1, V15.1.2, V16.0, V16.0.2, V16.1	Apply the hotfix https://internal.support.sw.siemens.com/en-US/knowledge-base/PL8602057 See further recommendations from section Workarounds and Mitigations

Tecnomatix eBOP Manager Server: V16.0.1, V16.1.1, V16.1.2	Currently no remediation is available Find detailed remediation and mitigation information at: https://internal.support.sw.siemens.com/en-US/knowledge-base/PL8602057 See further recommendations from section Workarounds and Mitigations
Tecnomatix Intosite: All versions	Vulnerabilities fixed on central cloud service; no user actions necessary See further recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation: V15.0, V16.0, V16.1	Currently no remediation is available Plant Simulation is only affected, when the TCCS (Teamcenter Client Communication System) is installed. Uninstall the TCCS. For details see: https://support.sw.siemens.com/knowledge-base/PL8600901 See further recommendations from section Workarounds and Mitigations
Tecnomatix Process Designer: All versions >= V14.1	Apply the hotfix, available for versions V14.1, V15.0, V15.1, V15.1.2, V16.0, V16.0.1, V16.0.2, V16.1, V16.1.1, V16.1.2 https://internal.support.sw.siemens.com/en-US/knowledge-base/PL8602057 See further recommendations from section Workarounds and Mitigations
Tecnomatix Process Simulate: All versions >= V14.1	Apply the hotfix, available for versions V14.1, V15.0, V15.1, V15.1.2, V16.0, V16.0.1, V16.0.2, V16.1, V16.1.1, V16.1.2 https://internal.support.sw.siemens.com/en-US/knowledge-base/PL8602057 See further recommendations from section Workarounds and Mitigations
Tecnomatix Process Simulate VCLite: All versions >= V14.1	Apply the hotfix, available for versions V14.1, V15.0, V15.1, V15.1.2, V16.0, V16.0.1, V16.0.2, V16.1, V16.1.1, V16.1.2 https://internal.support.sw.siemens.com/en-US/knowledge-base/PL8602057 See further recommendations from section Workarounds and Mitigations
Tecnomatix RobotExpert: All versions >= V14.1	Apply the hotfix, available for versions V14.1, V15.0, V15.1, V15.1.2, V16.0, V16.0.1, V16.0.2, V16.1, V16.1.1, V16.1.2 https://internal.support.sw.siemens.com/en-US/knowledge-base/PL8602057 See further recommendations from section Workarounds and Mitigations
Valor Parts Library - VPL Direct: V6.0, V6.1	Vulnerabilities fixed on remote VPL server; no user actions necessary See further recommendations from section Workarounds and Mitigations

Valor Parts Library - VPL Server or Service: V6.0, V6.1	Remove the JndiLookup class from the classpath. Find detailed remediation and mitigation information at: https://support.sw.siemens.com/knowledge-base/MG618362 See further recommendations from section Workarounds and Mitigations
VeSys: All versions >= 2019.1 SP1912 only if Teamcenter integration feature is used	Currently no remediation is available Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/MG618363 See further recommendations from section Workarounds and Mitigations
Xpedition Enterprise: All versions >= VX.2.6	A hotfix is available for versions VX.2.6, VX.2.7, VX.2.8, VX.2.10. Detailed instructions and download links are available at https://support.sw.siemens.com/en-US/product/1644094854/knowledge-base/MG618343 See further recommendations from section Workarounds and Mitigations
Xpedition IC Packaging: All versions >= VX.2.6	A hotfix is available for versions VX.2.6, VX.2.7, VX.2.8, VX.2.10. Detailed instructions and download links are available at https://support.sw.siemens.com/en-US/product/1644094854/knowledge-base/MG618343 See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- If the specific Siemens product allows it: Remove the JndiLookup class from the classpath: 'zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class'. This measure mitigates both CVE-2021-44228 and CVE-2021-45046. Note: in case you reinstall or update the product to a yet unfixed version later: check if the vulnerable JndiLookup class has to be removed again.
- If the specific Siemens product allows it: Update the Log4j component to 2.16.0 or later versions on the systems where the product is installed. This measure mitigates both CVE-2021-44228 and CVE-2021-45046. Note: in case you reinstall or update the product to a yet unfixed version later: check if the Log4j component has to be updated again.
- If, for a particular product listed in the table above, no remediation or specific mitigation is given: Block both incoming and outgoing connections between the system and the Internet.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Advantage Navigator is a cloud-based advanced analytics platform designed to help you optimize the performance of your buildings.

Aprisa is a route-centric physical design platform for the modern SoC.

Building Twin is a cloud-based software providing multi tenancy concepts and APIs for accessing building data of the digital replica of the building. Building Twin and 360° Viewer enables application development based on location aware building data including live data of the building. For digitization of brownfield buildings or documentation of the progress during construction the NavVis IVION Viewer utilizes the combination of 360° panoramic images with highly precise point clouds created by laser scans.

CADRA is a unique portfolio of affordable, easy-to-use 2.5D drafting software that allows you to reuse existing geometry within a drawing.

Calibre Design Solutions delivers a complete IC verification and DFM optimization platform. Calibre IC Manufacturing products ensure fast ramp and maximum process yield through the entire technology node life cycle.

Catapult provides solutions for High-Level Synthesis and Verification via C++ and SystemC language support, FPGA and ASIC independence and more.

Comfy is a workplace experience app that gives employees personal control, while delivering operational results for workplace teams.

COMOS is a unified data platform for collaborative plant design, operation and management that supports collecting, processing, saving, and distributing of information throughout the entire plant lifecycle.

Connect X200 Gateways are designed to connect building devices to cloud applications such as Building Operator or Cerberus Cloud Apps through the internet.

Connect X300 Gateways are designed to connect building devices to cloud applications such as Building Operator or Cerberus Cloud Apps through the internet.

cRSP (common Remote Service Platform) provides system-specific access and remote services for automation systems.

E-Car OC (E-Car Operation Center) is a cloud service that manages charging infrastructures for electric vehicles (EVs), both in domestic and public or semi-public areas.

EnergyIP applications enable utilities, retailers, DSO's and market operators proven technology to meet the needs and requirements of the energy sector.

EnergyIP Prepay is an end-to-end solution for smart prepaid energy management. It features flexible tariff management, real-time rating and charging, convenient payment, and recharging options as well as intelligent energy consumption control features.

Enlighted Amaze is a back-end service for the cloud-based Enlighted applications.

Enlighted Manage is available as a cloud-based software or on-premise server stores, performs analysis, and provides visual reporting of sensor data. In addition to being the collection point for energy, occupancy, and environmental data captured by the Enlighted Sensors, Manage provides a web-based user interface for lighting system management, IoT device management, and optimizing building system performance.

Enlighted Where application reliably locates people and assets in real-time in a building or across buildings anywhere in an enterprise.

FIN Framework (FIN) is a software framework with application suites that can integrate, control, manage, analyze, visualize and connect.

Geolus Shape Search is a geometry-based 3D search engine for both single and multi-CAD environment PLM stakeholders.

HES UDIS (Head-End System Universal Device Integration System) is an integrated solution for processing meter data and device events.

HyperLynx provides integrated signal integrity, power integrity, 3D electromagnetic modeling & electrical rule checking for high-speed digital PCB designs.

Industrial Edge Management (IEM) enables a centralized management of Siemens Industrial Edge Devices and Edge Applications. IEM is tailored to customer's needs and is operated by the customer (on-premises).

jROS (joint Resource Optimization and Scheduler) is a collection of forecasting and planning applications for the energy market. It is designed as a shared component of Spectrum Power. It may also be used as a stand-alone planning system or integrated in a SCADA/EMS System.

LOGO! Soft Comfort is an engineering software to configure and program LOGO! BM (Base Module) devices.

Mendix is a high productivity app platform that enables you to build and continuously improve mobile and web applications at scale. The Mendix Platform is designed to accelerate enterprise app delivery across your entire application development lifecycle, from ideation to deployment and operations.

MindSphere Asset Manager can be used to onboard and offboard agents to your account, configure assets, asset types and aspect types.

MindSphere Cloud Foundry Org is an environment to host, test and operate applications.

MindSphere Developer Cockpit can be used to manage your applications. MindSphere Operator Cockpit can be used to transfer applications from a Developer Cockpit, deploy the Cloud Foundry applications, register self-hosted applications, etc.

MindSphere Identity and Access Management are services available via their respective MindSphere APIs. These services are used to manage users, customers/subtenants, roles and scopes.

MindSphere Integrated Data Lake allows you to store data as an object, bring together data from different sources and use it with applications and tools. You can organize data in different folders, associate it with metadata tags, search and delete objects.

MindSphere is the leading industrial IoT as a service solution. Using advanced analytics and AI, MindSphere powers IoT solutions from the edge to the cloud with data from connected products, plants and systems to optimize operations, create better quality products and deploy new business models.

MindSphere Notification Service is available via its respective MindSphere APIs. This service enables you to send emails, mobile push notifications and SMS in relation to certain events defined by you or send email notifications to (a group of) individual recipients.

MindSphere Predictive Learning allows you to build predictive models through machine learning techniques, enabling companies to optimize product quality as well as reduce potential field failures and performance issues. You can employ diverse machine learning algorithms. It also allows you to build and execute predictive models in Python, R and Spark.

MindSphere Usage Transparency Service is a service available via its respective MindSphere APIs. This service offers insight on your consumption of certain resources and corresponding limits of your MindAccess plans and other subscribed services, e.g., API calls, number of users, inbound traffic and data storage volume. Moreover, developers can define metrics within this service so that consumption can be tracked.

MindSphere Visual Explorer enables you to visualize certain parts of your content. Such visualizations can be combined into dashboards, which may be used to analyse the performance of connected assets.

NX software is an integrated toolset that helps to develop design, simulation, and manufacturing solutions by supporting various aspects of product development allowing the designer to optimize shape to achieve a multidisciplinary design.

NXpower Monitor is a cloud-based application to start and accompany your digital journey in energy distribution. It enables you to monitor and visualize your electrical assets throughout the world at all times and from any location.

Opcenter APS (formerly known as "Preactor APS") is a family of production planning and scheduling software products that help you better orchestrate manufacturing processes.

Opcenter Intelligence (formerly known as “Manufacturing Intelligence”) connects, organizes and aggregates manufacturing data from disparate company sources into cohesive, intelligent and contextualized information.

Operation Scheduler is a tool that enables security operators to intelligently perform routine tasks. It can be used to schedule maintenance tasks.

PADS Professional is an integrated PCB design and verification flow for hardware engineers and small workgroups that delivers compatibility with Xpedition technology and extended collaboration for PCB engineering projects.

PADS Standard and Standard Plus provide PCB schematic design and layout capabilities in an intuitive and easy-to-use environment.

PartQuest is a cloud-based design, modeling, simulation, and analysis environment for electronic and mechatronic circuits and systems.

SENTRON powermanager power monitoring software analyzes energy consumption by displaying important characteristics for individual devices and for the entire system on an easy-to-understand dashboard.

SIGUARD DSA is a model-based dynamic stability assessment tool for online control room use and offline operational planning purposes.

SIMATIC IPC (Industrial PC) is the hardware platform for PC-based Automation from Siemens.

SIMATIC IT Report Manager provides a set of tools for reporting, composed of engineering tools and runtime tools.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

Simcenter 3D is a comprehensive, fully-integrated CAE solution for complex, multidisciplinary product performance engineering.

Simcenter System Simulation Client for Git provides a smart way of day-to-day versioning of systems simulation architecture, models and libraries.

Simcenter Testlab is a complete, integrated solution for test-based engineering, combining high-speed multi-physics data acquisition with a full suite of integrated testing, analytics, and modeling tools for a wide range of test needs.

SiPass integrated is a powerful and extremely flexible access control system.

Siveillance Control Pro is a command and control solution, specifically designed to support security management at critical infrastructure sites such as ports, airports, oil and gas power generation and distribution, chemical and pharma industries, heavy industries and campus environments.

Siveillance Vantage is an innovative and advanced software solution for mission critical security command and control centers operating critical infrastructure applications.

Solid Edge CAM Pro is a modular, flexible configuration of numerical control (NC) programming solutions.

Solid Edge Harness Design is a graphical design application for creating harness and formboard drawings.

Solid Edge is a portfolio of software tools that addresses various product development processes: 3D design, simulation, manufacturing and design management.

Spectrum Power provides basic components for SCADA, communications, and data modeling for control and monitoring systems. Application suites can be added to optimize network and generation management for all areas of energy management.

Teamcenter Active Workspace is a web application for accessing the Teamcenter system that provides an identical and seamless experience on any computer or smart device.

Teamcenter Briefcase Browser is an easy to use tool for suppliers that do not have Teamcenter. The browser can run on a supplier’s desktop and enables suppliers to exchange CAD design data.

Teamcenter Data Share Manager simplifies the upload and download of large files, including CAD designs.

Teamcenter Deployment Center is a web based installer that helps to easily install, patch, and upgrade Teamcenter software across a various other environments.

Teamcenter EDA allows to edit and release design variants where users can map item attributes to the associated variant and generate a BOM appropriate for each design variant.

Teamcenter File Management System (FMS) is used for managing files or vault in Teamcenter. FMS is responsible for all transaction related to files from Teamcenter server and client.

Teamcenter Integration for CATIA enhances your CATIA environment with a full range of product lifecycle management (PLM) capabilities.

Teamcenter Integration Framework (TcIF) integrates Teamcenter with other systems, helping to automate processes which cross system boundaries.

Teamcenter MBSE (model-based systems engineering) is a critical part of Teamcenter product lifecycle management (PLM) that allows to do multi-domain product development.

Teamcenter Polarion Integration is an integrated ALMPLM solution that effectively merges the advanced software application development capabilities of Polarion.

Teamcenter Rapid Start provides computer-aided design (CAD) data management capabilities for multi-CAD, mechanical CAD (MCAD) and electronic CAD (ECAD) that enable you to effectively manage, control and share design data across your entire design and supply chain.

Teamcenter Reporting and Analytics is a collaborative real-time or near realtime business intelligence/analytics (BI) product.

Teamcenter Requirements Integrator allows to import and exchange data with DOORS or RIF/ReqIF (requirements interchange format).

Teamcenter Retail Footwear and Apparel provides buyers, designers, technical designers, merchandisers and senior management with a central location to capture new trends, collaborate across the supply chain, and effectively manage the fashion product development process.

Teamcenter Security Services provides security solutions that are reliable and easily deployed and maintained across your lifecycle management processes.

Teamcenter software is a modern, adaptable product lifecycle management (PLM) system that connects people and processes, across functional silos, with a digital thread for innovation.

Teamcenter Structured Content Management and Technical Publishing suite helps for automating the activities associated with authoring, assembling and publishing complex product and/or service documentation in multiple languages and delivery formats.

Teamcenter Supplier Collaboration helps to collaborate with suppliers through interactions including Design Data Exchange, Direct Materials Sourcing, and Supplier Program Management.

Teamcenter System Modeling Workbench provides an integrated systems engineering environment that companies can use to apply standard model-based systems engineering (MBSE) concepts to the entire product development process.

Tecnomatix eBOP Manager Server is part of the Tecnomatix digital manufacturing solutions. It is built on the concept of the electronic bills of processes (eBOP) which manages product operations and resources.

Tecnomatix Intosite allows you to create cloud-based 2D/3D/panoramic representations of a production facility, presented in its geographical context.

Tecnomatix Plant Simulation allows you to model, simulate, explore and optimize logistics systems and their processes. These models enable analysis of material flow, resource utilization and logistics for all levels of manufacturing planning from global production facilities to local plants and specific lines, well in advance of production execution.

Tecnomatix Process Designer allows you to associate and reconcile multiple configurations of product bills of material (EBOMs), manufacturing bills of material (MBOMs), and bills of process (BOPs). You can also validate manufacturing planning decisions by using advanced visualization and analytical tools.

Tecnomatix Process Simulate is a digital manufacturing solution for manufacturing process verification in a 3D environment.

Tecnomatix RobotExpert is an easy-to-deploy, robot simulation and offline programming software that enables you to perform complete 3D modeling, visualization and simulation of your automation systems including robots, tooling and peripheral equipment.

Tecnomatix Unicam and Test Expert products provide Manufacturing Process Management (MPM) solutions for electronics manufacturers.

Tessent Silicon Lifecycle Solutions consists of products for IC test and functional monitoring, including best-in-class design-for-test tools and test data analytics, security, debug and in-life monitoring products that help ensure the highest test coverage, accelerate yield ramp and improve quality and reliability across the silicon lifecycle.

Valor NPI (new product introductions) brings DFM (design for manufacturability) into PCB layout/design, where issues can be discovered and corrected quickly and inexpensively instead of finding issues after handoff to manufacturing.

Valor Parts Library (VPL) connects PCB design to design-for-manufacturing (DFM), speeding up the new product introduction (NPI) process. Comprehensive DFM analysis of a PCB design can be performed using VPL and Valor NPI. VPL enables concurrent engineering for Valor NPI and Xpedition.

Veloce hardware-assisted verification system is used for the rapid verification of highly sophisticated, next-generation integrated circuit (IC) designs.

VeSys is a suite of wiring and harness design software tools.

Xpedition is an innovative PCB design flow application, providing integration from system design definition to manufacturing execution.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2021-44228

Apache Log4j V2, versions < 2.15.0 do not protect JNDI features (as used in configuration, log messages, and parameters) against attacker controlled LDAP and other JNDI related endpoints.

An attacker who can control log messages or log message parameters could execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-45046

The fix to address CVE-2021-44228 was incomplete in certain non-default configurations, when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, ${ctx:loginId}).

This could allow attackers with control over Thread Context Map (MDC) input data to craft malicious input data using a JNDI Lookup pattern, resulting in an information leak and remote code execution in some environments and local code execution in all environments.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

This advisory will be updated as more information becomes available.

Products Under Investigation:

The following Siemens products are under active investigation to determine whether they are affected:

- SIMATIC IT Report Manager V6.7 (for current status of investigation see https://support.sw.siemens.com/en-US/knowledge-base/PL8600875)
- cRSP Operator Client Starter

Non-exhaustive List of Products Currently Considered As Not Affected:

In particular, the following Siemens products are currently considered as not affected:

- Advantage Navigator Software Proxy V5
- Analog/Mixed Signal (AMS) products
- Aprisa
- CADRA
- Calibre products
- Catapult products
- Comfy
- cRSP
- Desigo Insight
- Enlighted: eCloud, Safe, Space, Manage in the Cloud, People Counting, Gateways and Sensors
- Enlighted Manage (detailed explanation at https://support.enlightedinc.com/hc/en-us/articles/4414353643667-Log4J-Vulnerability)
- FIN Framework
- HyperLynx
- IC Flow (Tanner, Pyxis, LightSuite Photonic Compiler)
- LOGO! products
- Opcenter APS
- PADS Standard, Standard Plus, Professional
- PartQuest
- Polarion
- Reyrolle products
- RUGGEDCOM products
- SCALANCE products
- SICAM products
- SIDRIVE IQ products
- SIGUARD PDP
- SIMATIC products (except for a subset of SIMATIC IPCs)
- SIMOTICS CONNECT 600
- SINAMICS products
- SINAMICS MV products
- SINUMERIK products

- Simcenter FloTHERM PACK and Flomaster
- SIPROTEC products
- SiPass integrated, versions < V2.80
- Siveillance Video
- Siveillance Viewpoint
- Solido products
- Tecnomatix Unicam and Test Expert products
- Tessent products
- Valor NPI
- Veloce (Veloce, Prototyping System, Certus, VIPR, Software Debug, System Level Analysis, Vista, X-STEP)
- Xpedition Valydate

As mentioned above, this is an ongoing investigation. Thus, products that are currently considered as not affected may subsequently be considered as affected when additional information becomes available.

Errata:

The following products were temporarily listed as affected. They were removed after closer investigation showed that they are not affected:

- SIMATIC WinCC, all versions (V7.4 was listed as affected in V1.0-V1.1 of the advisory)
- LOGO! Soft Comfort (listed as affected in V1.0-V1.2 of the advisory)
- Siveillance Viewpoint (listed as affected in V1.2-V1.3 of the advisory)
- Connect X200/X300 gateways (listed as affected in V1.5 of the advisory; only the Building Operator Discovery applications are affected, not the gateways themselves)

Additional Notes:

For the impact of the Log4j vulnerabilities to solutions provided by Siemens Mobility and Affiliates please address your local service or sales contact.

Note: two additional vulnerabilities were published for Apache Log4j, the impact of which are documented in SSA-501673: https://cert-portal.siemens.com/productcert/pdf/ssa-501673.pdf (CVE-2021-45105) and SSA-784507: https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf (CVE-2021-44832).

For more details regarding the Log4j vulnerabilities refer to https://logging.apache.org/log4j/2.x/security.html

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2021-12-13): Publication Date
V1.1 (2021-12-15): Added additional (potentially) affected products and additional remediation or mitigation measures; added reference to CVE-2021-45046 and updated mitigations accordingly
V1.2 (2021-12-16): Added additional affected products, remediation or mitigation measures, and products under investigation; removed SIMATIC WinCC V7.4 because it is not affected
V1.3 (2021-12-17): Added additional affected products, remediation or mitigation measures, and products under investigation; removed LOGO! Soft Comfort because it is not affected; expanded Teamcenter Suite to individual affected applications in Teamcenter; updated information for Desigo CC and Cerberus DMS
V1.4 (2021-12-18): Revised severity of CVE-2021-45046 and removed ineffective mitigation measures; added Comfy and Enlighted; added individual Mindsphere applications; removed Siveillance Viewpoint because it is not affected; added a statement regarding Siemens Mobility solutions
V1.5 (2021-12-19): Added reference to new SSA-501673 that covers a new Log4j vulnerability (CVE-2021-45105); added remediation for SENTRON powermanager V4; added Connect X200/X300 gateways
V1.6 (2021-12-20): Added non-exhaustive list of Siemens products currently not considered as affected; updated information for Industrial Edge Management OS and for SENTRON powermanager; updated impact, mitigation measures and fix release information for EnergyIP Prepay; added remediation for SIGUARD DSA; clarified Building Operator Discovery Applications vs. Connect X200/X300 gateways; added remediation for Advantage Navigator Software Proxy V6; added Advantage Navigator Software Proxy V5 to list of not affected products
V1.7 (2021-12-21): Added solution for MindSphere Visual Explorer; added jROS for Spectrum Power, Building Twin - 360° Viewer, and NXpower Monitor; added additional products considered as not affected
V1.8 (2021-12-22): Added Simcenter Testlab and Teamcenter Integration for CATIA; added additional products considered as not affected
V1.9 (2021-12-23): Added solution for MindSphere Predictive Learning, GMA-Manager, Operation Scheduler, and Siveillance Identity; added SIMATIC IT Report Manager, Simcenter System Simulation Client for Git, Tecnomatix Intosite, Tecnomatix Plant Simulation, and Valor Parts Library; added additional products considered as not affected; updated section “Workarounds and Mitigations”
V2.0 (2021-12-27): Added solution for Xpedition Enterprise and IC Packaging; updated information for Geolus Shape Search; added SIMATIC IPCs as under investigation; added additional products considered as not affected
V2.1 (2021-12-28): Added SIMATIC IPCs with Adaptec RAID; added additional Tecnomatix products (Process Designer, Process Simulate, RobotExpert, eBOP Manager Server); added reference to new SSA-784507 that covers a new Log4j vulnerability (CVE-2021-44832)
V2.2 (2022-01-05): Added solution for Simcenter 3D, and for Tecnomatix eBOP Manager Server V15.0, V16.0.2; added cRSP Operator Client Starter as under investigation; added a note regarding Enlighted Manage

TERMS OF USE

additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.