Advisory Alert

Alert Number: AAA20251210 **Date:** December 10, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Stack-Based Buffer Overflow Vulnerability
Ivanti	**Critical**	Stored Cross-Site Scripting Vulnerability
Fortinet	**Critical**	An Improper Verification of Cryptographic Signature Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Fortinet	**High**	Multiple Vulnerabilities
SAP	**High, Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Intel	**Low**	Multiple Vulnerabilities
AMD	**Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Stack-Based Buffer Overflow Vulnerability (CVE-2025-30472)
Description	IBM has released security updates addressing a Stack-Based Buffer Overflow Vulnerability that exists in IBM DB2. **CVE-2025-30472** - A stack-based buffer overflow vulnerability in the corosync library (specifically in orf_token_endian_convert in exec/totemsrp.c). This issue arises if encryption is disabled or if an attacker possesses the encryption key, allowing for potential exploitation via a large UDP packet. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7240977

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Stored Cross-Site Scripting Vulnerability (CVE-2025-10573)
Description	Ivanti has released a security update addressing a Stored Cross-Site Scripting Vulnerability that exists in Ivanti Endpoint Manager (EPM). **CVE-2025-10573 -** A remote attacker, without needing to log in, can plant malicious code (XSS) on the EPM server. Upon an administrator's interaction with the contaminated section of the EPM console, the code executes, allowing the attacker to hijack their session and potentially gain full administrative control. Ivanti advises to upgrade to the fixed version at your earliest to protect systems from potential threats. Furthermore, for immediate action Ivanti advises keeping its EPM management interface isolated as it is not intended to be an internet-facing solution.
Affected Products	Ivanti Endpoint Manager 2024 SU4 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-EPM-December-2025-for-EPM-2024?language=en_US

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	An Improper Verification of Cryptographic Signature Vulnerability (CVE-2025-59718, CVE-2025-59719)
Description	Fortinet has released security updates addressing An Improper Verification of Cryptographic Signature Vulnerability that exist in FortiOS, FortiProxy, FortiSwitchManager and FortiWeb. **CVE-2025-59718 / CVE-2025-59719 -** An unauthenticated, remote attacker can craft a malicious SAML message that the vulnerable Fortinet device accepts as legitimate, allowing the attacker to bypass the login process and gain administrative access. This vulnerability is only exploitable if FortiCloud Single Sign-On (SSO) login feature is enabled. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiOS 7.6.0 - 7.6.3 FortiOS 7.4.0 - 7.4.8 FortiOS 7.2.0 - 7.2.11 FortiOS 7.0.0 - 7.0.17 FortiProxy 7.6.0 - 7.6.3 FortiProxy 7.4.0 - 7.4.10 FortiProxy 7.2.0 - 7.2.14 FortiProxy 7.0.0 - 7.0.21 FortiSwitchManager 7.2.0 - 7.2.6 FortiSwitchManager 7.0.0 - 7.0.5 FortiWeb 8.0.0 FortiWeb 7.6.0 - 7.6.4 FortiWeb 7.4.0 - 7.4.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-25-647

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Windows Server 2025 (Server Core installation) • Windows Server 2025 • Windows Server 2022, 23H2 Edition (Server Core installation) • Windows Server 2022 (Server Core installation) • Windows Server 2022 • Windows Server 2019 (Server Core installation) • Windows Server 2019 • Windows Server 2016 (Server Core installation) • Windows Server 2016 • Windows Server 2012 R2 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2012 (Server Core installation) • Windows Server 2012 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) • Windows Server 2008 R2 for x64-based Systems Service Pack 1 • Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) • Windows Server 2008 for x64-based Systems Service Pack 2 • Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) • Windows Server 2008 for 32-bit Systems Service Pack 2 • Windows 11 Version 25H2 for x64-based Systems • Windows 11 Version 25H2 for ARM64-based Systems • Windows 11 Version 24H2 for x64-based Systems • Windows 11 Version 24H2 for ARM64-based Systems • Windows 11 Version 23H2 for x64-based Systems • Windows 11 Version 23H2 for ARM64-based Systems • Windows 11 Version 22H2 for x64-based Systems • Windows 11 Version 22H2 for ARM64-based Systems • Windows 10 Version 22H2 for x64-based Systems • Windows 10 Version 22H2 for ARM64-based Systems • Windows 10 Version 22H2 for 32-bit Systems • Windows 10 Version 21H2 for x64-based Systems • Windows 10 Version 21H2 for ARM64-based Systems • Windows 10 Version 21H2 for 32-bit Systems • Windows 10 Version 1809 for x64-based Systems • Windows 10 Version 1809 for 32-bit Systems • Windows 10 Version 1607 for x64-based Systems • Windows 10 Version 1607 for 32-bit Systems • Windows 10 for x64-based Systems • Windows 10 for 32-bit Systems • Office Online Server • Microsoft Word 2016 (64-bit edition) • Microsoft Word 2016 (32-bit edition) • Microsoft SharePoint Server Subscription Edition • Microsoft SharePoint Server 2019 • Microsoft SharePoint Enterprise Server 2016 • Microsoft Office LTSC for Mac 2024 • Microsoft Office LTSC for Mac 2021 • Microsoft Office LTSC 2024 for 64-bit editions • Microsoft Office LTSC 2024 for 32-bit editions • Microsoft Office LTSC 2021 for 64-bit editions • Microsoft Office LTSC 2021 for 32-bit editions • Microsoft Office for Android • Microsoft Office 2019 for 64-bit editions • Microsoft Office 2019 for 32-bit editions • Microsoft Office 2016 (64-bit edition) • Microsoft Office 2016 (32-bit edition) • Microsoft Exchange Server Subscription Edition RTM • Microsoft Exchange Server 2019 Cumulative Update 15 • Microsoft Exchange Server 2019 Cumulative Update 14 • Microsoft Exchange Server 2016 Cumulative Update 23 • Microsoft Excel 2016 (64-bit edition) • Microsoft Excel 2016 (32-bit edition) • Microsoft Edge (Chromium-based) • Microsoft Access 2016 (64-bit edition) • Microsoft Access 2016 (32-bit edition) • Microsoft 365 Apps for Enterprise for 64-bit Systems • Microsoft 365 Apps for Enterprise for 32-bit Systems • GitHub Copilot Plugin for JetBrains IDEs • cbl2 kata-containers 3.2.0.azl2-7 • cbl2 python-tensorboard 2.11.0-3 • cbl2 vim 9.1.1616-1 • cbl2 tensorflow 2.11.1-2 • cbl2 syslinux 6.04-10 • cbl2 reaper 3.1.1-21 • cbl2 reaper 3.1.1-19 • cbl2 qt5-qtdeclarative 5.12.5-5 • cbl2 qt5-qtbase 5.12.11-18 • cbl2 python3 3.9.19-17 • cbl2 python3 3.9.19-16 • cbl2 prometheus 2.37.9-5 • cbl2 pgbouncer 1.24.1-1 • cbl2 msft-golang 1.24.9-1 • cbl2 msft-golang 1.24.11-1 • cbl2 moby-compose 2.17.3-12 • cbl2 moby-buildx 0.7.1-26 • cbl2 local-path-provisioner 0.0.21-19 • cbl2 libpng 1.6.51-1 • cbl2 libcontainers-common 20210626-7 • cbl2 kubevirt 0.59.0-31 • cbl2 kube-vip-cloud-provider 0.0.2-23 • cbl2 kubernetes 1.28.4-19 • cbl2 kernel 5.15.186.1-1 • cbl2 kata-containers-cc 3.2.0.azl2-8 • cbl2 jx 3.2.236-23 • cbl2 influxdb 2.6.1-24 • cbl2 httpd 2.4.65-1 • cbl2 golang 1.22.7-5 • cbl2 golang 1.18.8-10 • cbl2 gcc 11.2.0-9 • cbl2 gcc 11.2.0-8 • cbl2 flannel 0.14.0-26 • cbl2 dcos-cli 1.2.0-22 • cbl2 cri-o 1.22.3-17 • cbl2 containerized-data-importer 1.55.0-26 • cbl2 cni-plugins 1.3.0-9 • cbl2 cf-cli 8.4.0-25 • cbl2 cert-manager 1.11.2-24 • Azure Monitor Agent • azl3 vim 9.1.1616-1 • azl3 tensorflow 2.16.1-9 • azl3 syslinux 6.04-11 • azl3 qtdeclarative 6.6.1-1 • azl3 qtbase 6.6.3-4 • azl3 python-tensorboard 2.16.2-6 • azl3 python3 3.12.9-6 • azl3 python3 3.12.9-5 • azl3 pgbouncer 1.24.1-1 • azl3 libpng 1.6.40-1 • azl3 libcontainers-common 20240213-3 • azl3 kubernetes 1.30.10-16 • azl3 kernel 6.6.117.1-1 • azl3 kernel 6.6.112.1-2 • azl3 keras 3.3.3-5 • azl3 kata-containers-cc 3.15.0.aks0-5 • azl3 kata-containers 3.19.1.kata2-2 • azl3 influxdb 2.7.5-8 • azl3 httpd 2.4.65-1 • azl3 golang 1.25.5-1 • azl3 golang 1.25.3-1 • azl3 golang 1.23.12-1 • azl3 gcc 13.2.0-7 • azl3 flannel 0.24.2-21 • azl3 dcos-cli 1.2.0-19 • azl3 containerized-data-importer 1.57.0-17 • azl3 cni-plugins 1.4.0-3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42880, CVE-2025-42928, CVE-2025-55754)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-42880** - Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confidentiality, integrity and availability of the system. **CVE-2025-42928** - Under certain conditions, a high privileged user could exploit a deserialization vulnerability in SAP jConnect to launch remote code execution. The system may be vulnerable when specially crafted input is used to exploit the vulnerability resulting in high impact on confidentiality, integrity and availability of the system. **CVE-2025-55754** - Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat. Tomcat did not escape ANSI escape sequences in log messages. If Tomcat was running in a console on a Windows operating system, and the console supported ANSI escape sequences, it was possible for an attacker to use a specially crafted URL to inject ANSI escape sequences to manipulate the console and the clipboard and attempt to trick an administrator into running an attacker controlled command. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP Solution Manager version ST 720 SAP Commerce Cloud versions HY_COM 2205, COM_CLOUD 2211, COM_CLOUD 2211-JDK21 SAP jConnect - SDK for ASE versions SYBASE_SOFTWARE_DEVELOPER_KIT 16.0.4, 16.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2025.html

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-47319, CVE-2024-38798, CVE-2025-47323)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-47319** - A High-severity flaw in Qualcomm's High-Level Operating System (HLOS) component, which allows a local authenticated attacker to access sensitive data structures, leading to unauthorized Information Disclosure and potential privilege escalation. **CVE-2024-38798** - A flaw in the underlying EDK2 (UEFI firmware) code, which can allow a local attacker to achieve Escalation of Privilege (EoP) and execute arbitrary code within the highly trusted firmware. **CVE-2025-47323** - an Integer Overflow or Wraparound in the Qualcomm Audio component software. Where a memory corruption during packet processing, can be exploited by a local attacker to achieve Escalation of Privilege (EoP) and lead to a complete compromise of the system's confidentiality, integrity, and availability. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-207909

Affected Product	**Fortinet**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-64447, CVE-2025-53949, CVE-2025-60024)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-64447** - an unauthenticated attacker can submit a crafted HTTP or HTTPS request with forged cookies, and with prior knowledge of the target FortiWeb appliance's serial number, an attacker can execute arbitrary operations on the system, leading to an escalation of privilege. **CVE-2025-53949** – An OS Command Injection vulnerability, affecting multiple endpoints in FortiSandbox allows an attacker who has successfully authenticated to the system to exploit it by sending specifically crafted HTTP requests. Successful exploitation allows the attacker to execute unauthorized code or commands on the underlying FortiSandbox system. **CVE-2025-60024** - A Path Traversal flaw residing in the administrative interface of FortiVoice, allows a privileged attacker who is already authenticated to the system to write arbitrary files to the file system. The attack is carried out by sending specifically crafted HTTP or HTTPS commands and can lead to a critical escalation of privilege. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiWeb Versions 8.0.0 - 8.0.1 FortiWeb Versions 7.6.0 - 7.6.5 FortiWeb Versions 7.4.0 - 7.4.10 FortiWeb Versions 7.2.0 - 7.2.11 FortiWeb Versions 7.0.0 - 7.0.11 FortiSandbox Versions 5.0.0 - 5.0.2 FortiSandbox Versions 4.4.0 - 4.4.7 FortiSandbox Versions 4.2.x (All versions) FortiSandbox Versions 4.0.x (All versions) FortiVoice Versions 7.2.0 - 7.2.2 FortiVoice Versions 7.0.0 - 7.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-25-945 • https://www.fortiguard.com/psirt/FG-IR-25-479 • https://www.fortiguard.com/psirt/FG-IR-25-812

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42872, CVE-2025-42873, CVE-2025-42874, CVE-2025-42875, CVE-2025-42876, CVE-2025-42877, CVE-2025-42891, CVE-2025-42896, CVE-2025-42904, CVE-2025-48976)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of service, Sensitive Data Exposure, Memory Corruption, Cross-site Scripting, Server-Side Request Forgery. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Web Dispatcher and Internet Communication Manager (ICM) versions KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, WEBDISP 7.22_EXT, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16 • SAP NetWeaver (remote service for Xcelsius) versions BI-BASE-E 7.50, BI-BASE-B 7.50, BI-IBC 7.50, BI-BASE-S 7.50, BIWEBAPP 7.50 • SAP Business Objects versions ENTERPRISE 430, 2025, 2027 • SAP Web Dispatcher, Internet Communication Manager and SAP Content Server version(s) KRNL64UC 7.53, WEBDISP 7.53, 7.54, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1, CONTSERV 7.53, 7.54, KERNEL 7.53, 7.54 • SAP S/4 HANA Private Cloud (Financials General Ledger) versions S4CORE 104, 105, 106, 107, 108, 109 • SAP NetWeaver Internet Communication Framework versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 • Application Server ABAP versions - KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.17 • SAP NetWeaver Enterprise Portal versions EP-RUNTIME 7.50 • SAPUI5 framework (Markdown-it component) versions SAP_UI 755, 756, 757, 758 • SAP Enterprise Search for ABAP versions SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816 • SAP BusinessObjects Business Intelligence Platform versions ENTERPRISE 430, 2025, 2027
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2025.html

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-36006, CVE-2025-33012, CVE-2025-2534, CVE-2025-33134, CVE-2025-2533)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2. These vulnerabilities could be exploited by malicious users to cause denial of service and gain unauthorized access. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Versions 12.1.0 - 12.1.3 IBM Db2 Versions 11.5.0 - 11.5.9 IBM Db2 Versions 11.1.0 - 11.1.4.7 IBM Db2 Versions 10.5.0 - 10.5.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7250479 • https://www.ibm.com/support/pages/node/7250469 • https://www.ibm.com/support/pages/node/7250472 • https://www.ibm.com/support/pages/node/7250470 • https://www.ibm.com/support/pages/node/7240947

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3640, CVE-2025-38718, CVE-2023-53305, CVE-2022-50341, CVE-2023-53365, CVE-2022-50386, CVE-2022-50408)
Description	Red Hat has released security updates for the kernel packages in Red Hat Enterprise Linux 7 Extended Lifecycle Support. These updates address multiple vulnerabilities, including several use-after-free flaws in the Bluetooth L2CAP and Wi-Fi subsystems, a denial of service vulnerability in SCTP, and crash issues in the CIFS and IP6MR components. Applying this kernel update is necessary to mitigate potential threats that could lead to system instability, denial of service, or other compromises.
Affected Products	• Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:22910

Affected Product	**AMD**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-9612, CVE-2025-9613, CVE-2025-9614)
Description	AMD has released Security updates addressing multiple vulnerabilities related to the PCI Express (PCIe) Integrity and Data Encryption (IDE) specification that affect some AMD EPYC™ processors. **CVE-2025-9612** - Replay/Reordering Vulnerability: Insufficient guidance in the PCIe IDE specification on Transaction Layer Packet (TLP) ordering and tag uniqueness may allow encrypted packets to be replayed or reordered without detection. This could be exploited by a local or physical attacker. **CVE-2025-9613** - Tag Aliasing Vulnerability: Insufficient guidance in the PCIe IDE specification on tag reuse after completion timeouts may allow multiple outstanding Non-Posted Requests to share the same tag. This can result in completions being delivered to the wrong security context, potentially compromising data integrity and confidentiality. **CVE-2025-9614** - Stale Write Transaction Vulnerability: Insufficient guidance on re-keying and stream flushing during device rebinding may allow stale write transactions from a previous security context to be processed in a new one. This can lead to unintended data compromise. AMD advises customers to apply the security updates for the affected processors to protect systems from potential threats.
Affected Products	AMD EPYC™ 9005 Series Processors AMD EPYC™ Embedded 9005 Series Processors
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7056.html

Affected Product	**Intel**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-9612, CVE-2025-9613, CVE-2025-9614)
Description	Intel has released a security updates addressing multiple vulnerabilities that exist in the design specifications for the PCI Express (PCIe) Integrity and Data Encryption (IDE) and the TEE Device Interface Security Protocol (TDISP), which are relevant to systems using Intel® Trust Domain Extensions Connect (Intel® TDX Connect). **CVE-2025-9613** – A Completion Timeout Redirection (CTR) vulnerability allows a malicious privileged software adversary to induce Completion timeouts in PCIe IDE traffic. This may cause Completions (responses to read requests) intended for one Trust Domain (TD) to be redirected to a second TD, potentially leading to confidentiality violation of the data. **CVE-2025-9614** – A Delayed Posted Redirection (DPR) vulnerability allows Posted Requests to be delayed by a malicious programmable PCIe switch until the destination TEE Device Interface (TDI) is re-bound to a different TD. The delayed PRs may result in confidentiality and integrity compromise. **CVE-2025-9612** – A Forbidden IDE Reordering (FIR) vulnerability in the PCIe IDE may allow read requests to bypass write requests in certain circumstances. This could cause the requester to unknowingly consume stale data, leading to an integrity violation. Intel advises customers not to use programmable PCIe switches in Intel TDX Connect and IDE deployments involving affected processors. Additionally, Virtual Machine Monitor (VMM) updates are recommended to refresh IDE key(s) used by a device function before re-assigning it to a different VM or TD to mitigate the DPR issue.
Affected Products	Intel® Xeon® 6 Processors with P-cores Intel® Xeon® 6700P-B/6500P-B series SoC with P-Cores
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01409.html

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.