Filters

What are you looking for?

Date Added (optional)

Sort by (optional)

Date Added

Items per page (optional)

20

APPLY

Vendor/Project

Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

HOW TO USE THE KEV CATALOG

The KEV catalog is also available in these formats:

CSV

JSON

JSON Schema (updated 06-25-2024)

Print View

License

Showing 1 - 20 of 1302

APPLE | MULTIPLE PRODUCTS

CVE-2025-24201

Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability: *Apple iOS, iPadOS, macOS, and other Apple products contain an out-of-bounds write vulnerability in WebKit that may allow maliciously crafted web content to break out of Web Content sandbox. This vulnerability could impact HTML parsers that use WebKit, including but not limited to Apple Safari and non-Apple products which rely on WebKit for HTML processing.*

Related CWE: CWE-787

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-13
- **Due Date:** 2025-04-03

Additional Notes +

JUNIPER | JUNOS OS

CVE-2025-21590

Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability: *Juniper Junos OS contains an improper isolation or compartmentalization vulnerability. This vulnerability could allows a local attacker with high privileges to inject arbitrary code.*

Related CWE: CWE-653

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-13
- **Due Date:** 2025-04-03

Additional Notes +

MICROSOFT | WINDOWS

CVE-2025-26633

Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability: *Microsoft Windows Management Console (MMC) contains an improper neutralization vulnerability that allows an unauthorized attacker to bypass a security feature locally.*

Related CWE: CWE-707

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-11
- **Due Date:** 2025-04-01

Additional Notes +

MICROSOFT | WINDOWS

CVE-2025-24983

Microsoft Windows Win32k Use-After-Free Vulnerability: *Microsoft Windows Win32 Kernel Subsystem contains a use-after-free vulnerability that allows an authorized attacker to elevate privileges locally.*

Related CWE: CWE-416

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-11
- **Due Date:** 2025-04-01

Additional Notes +

MICROSOFT | WINDOWS

CVE-2025-24984

Microsoft Windows NTFS Information Disclosure Vulnerability: *Microsoft Windows New Technology File System (NTFS) contains an insertion of sensitive Information into log file vulnerability that allows an unauthorized attacker to disclose information with a physical attack. An attacker who successfully exploited this vulnerability could potentially read portions of heap memory.*

Related CWE: CWE-532

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-11
- **Due Date:** 2025-04-01

Additional Notes +

MICROSOFT | WINDOWS

CVE-2025-24985

Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability: *Microsoft Windows Fast FAT File System Driver contains an integer overflow or*

wraparound vulnerability that allows an unauthorized attacker to execute code locally.

Related CWEs: CWE-190 | CWE-122

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-11
- **Due Date:** 2025-04-01

Additional Notes +

MICROSOFT | WINDOWS

CVE-2025-24991

Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability: *Microsoft Windows New Technology File System (NTFS) contains an out-of-bounds read vulnerability that allows an authorized attacker to disclose information locally.*

Related CWE: CWE-125

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-11
- **Due Date:** 2025-04-01

Additional Notes +

MICROSOFT | WINDOWS

CVE-2025-24993

Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability: *Microsoft Windows New Technology File System (NTFS) contains a heap-based buffer overflow vulnerability that allows an unauthorized attacker to execute code locally.*

Related CWE: CWE-122

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or

- **Date Added:** 2025-03-11
- **Due Date:** 2025-04-01

discontinue use of the product if mitigations are unavailable.

Additional Notes +

ADVANTIVE | VERACORE

CVE-2025-25181

Advantive VeraCore SQL Injection Vulnerability: *Advantive VeraCore contains a SQL injection vulnerability in timeoutWarning.asp that allows a remote attacker to execute arbitrary SQL commands via the PmSess1 parameter.*

Related CWE: CWE-89

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-10
- **Due Date:** 2025-03-31

Additional Notes +

ADVANTIVE | VERACORE

CVE-2024-57968

Advantive VeraCore Unrestricted File Upload Vulnerability: *Advantive VeraCore contains an unrestricted file upload vulnerability that allows a remote unauthenticated attacker to upload files to unintended folders via upload.apsx.*

Related CWE: CWE-434

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-10
- **Due Date:** 2025-03-31

Additional Notes +

IVANTI | ENDPOINT MANAGER (EPM)

CVE-2024-13159

Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability: *Ivanti Endpoint Manager (EPM) contains an absolute path traversal vulnerability that*

allows a remote unauthenticated attacker to leak sensitive information.

Related CWE: CWE-36

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-10
- **Due Date:** 2025-03-31

Additional Notes +

IVANTI | ENDPOINT MANAGER (EPM)

CVE-2024-13160

Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability: *Ivanti Endpoint Manager (EPM) contains an absolute path traversal vulnerability that allows a remote unauthenticated attacker to leak sensitive information.*

Related CWE: CWE-36

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-10
- **Due Date:** 2025-03-31

Additional Notes +

IVANTI | ENDPOINT MANAGER (EPM)

CVE-2024-13161

Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability: *Ivanti Endpoint Manager (EPM) contains an absolute path traversal vulnerability that allows a remote unauthenticated attacker to leak sensitive information.*

Related CWE: CWE-36

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-10
- **Due Date:** 2025-03-31

Additional Notes +

LINUX | KERNEL

CVE-2024-50302

Linux Kernel Use of Uninitialized Resource Vulnerability: *The Linux kernel contains a use of uninitialized resource vulnerability that allows an attacker to leak kernel memory via a specially crafted HID report.*

Related CWE: CWE-908

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-04
- **Due Date:** 2025-03-25

Additional Notes +

VMWARE | ESXI AND WORKSTATION

CVE-2025-22224

VMware ESXi and Workstation TOCTOU Race Condition Vulnerability: *VMware ESXi and Workstation contain a time-of-check time-of-use (TOCTOU) race condition vulnerability that leads to an out-of-bounds write. Successful exploitation enables an attacker with local administrative privileges on a virtual machine to execute code as the virtual machine's VMX process running on the host.*

Related CWE: CWE-367

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-04
- **Due Date:** 2025-03-25

Additional Notes +

VMWARE | ESXI

CVE-2025-22225

VMware ESXi Arbitrary Write Vulnerability: *VMware ESXi contains an arbitrary write vulnerability. Successful exploitation allows an attacker with privileges within the VMX process to trigger an arbitrary kernel write leading to an escape of the sandbox.*

Related CWE: CWE-123

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-04
- **Due Date:** 2025-03-25

Additional Notes +

VMWARE | ESXI, WORKSTATION, AND FUSION

CVE-2025-22226

VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability: *VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. Successful exploitation allows an attacker with administrative privileges to a virtual machine to leak memory from the vmx process.*

Related CWE: CWE-125

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-04
- **Due Date:** 2025-03-25

Additional Notes +

CISCO | SMALL BUSINESS RV SERIES ROUTERS

CVE-2023-20118

Cisco Small Business RV Series Routers Command Injection Vulnerability: *Multiple Cisco Small Business RV Series Routers contains a command injection vulnerability in the web-based management interface. Successful exploitation could allow an authenticated, remote attacker to gain root-level privileges and access unauthorized data.*

Related CWE: CWE-77

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or

- **Date Added:** 2025-03-03
- **Due Date:** 2025-03-24

discontinue use of the product if mitigations are unavailable.

Additional Notes +

HITACHI VANTARA | PENTAHO BUSINESS ANALYTICS (BA) SERVER

CVE-2022-43939

Hitachi Vantara Pentaho BA Server Authorization Bypass Vulnerability: *Hitachi Vantara Pentaho BA Server contains a use of non-canonical URL paths for authorization decisions vulnerability that enables an attacker to bypass authorization.*

Related CWE: CWE-647

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-03
- **Due Date:** 2025-03-24

Additional Notes +

HITACHI VANTARA | PENTAHO BUSINESS ANALYTICS (BA) SERVER

CVE-2022-43769

Hitachi Vantara Pentaho BA Server Special Element Injection Vulnerability: *Hitachi Vantara Pentaho BA Server contains a special element injection vulnerability that allows an attacker to inject Spring templates into properties files, allowing for arbitrary command execution.*

Related CWE: CWE-74

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-03-03
- **Due Date:** 2025-03-24

Additional Notes +

1 2 3 4 5 6 7 8 9 … Next › Last »

Subscribe to the KEV Catalog Updates

Stay up to date on the latest known exploited vulnerabilities.

SUBSCRIBE NOW

Return to top

Topics Spotlight Resources & Tools News & Events Careers About

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov