



# Security Bulletin: Multiple Vulnerabilities in IBM Concert Software.

## Security Bulletin

### Summary

Multiple vulnerabilities were addressed in IBM Concert Software version 1.1.0

### Vulnerability Details

**CVEID:** [CVE-2024-55909](https://www.cve.org/CVERecord?id=CVE-2024-55909) (<https://www.cve.org/CVERecord?id=CVE-2024-55909>)

**DESCRIPTION:** IBM Concert Software could allow an authenticated user to cause a denial of service due to the expansion of archive files without controlling resource consumption.

**CWE:** [CWE-409: Improper Handling of Highly Compressed Data \(Data Amplification\)](https://cwe.mitre.org/data/definitions/409.html)

(<https://cwe.mitre.org/data/definitions/409.html>)

**CVSS Source:** IBM

**CVSS Base score:** 6.5

**CVSS Vector:** (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

**CVEID:** [CVE-2024-6119](https://www.cve.org/CVERecord?id=CVE-2024-6119) (<https://www.cve.org/CVERecord?id=CVE-2024-6119>)

**DESCRIPTION:** Issue summary: Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process. Impact summary: Abnormal termination of an application can cause a denial of service. Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address when comparing the expected name with an `otherName` subject alternative name of an X.509 certificate. This may result in an exception that terminates the application program. Note that basic certificate chain validation (signatures, dates, ...) is not affected, the denial of service can occur only when the application also specifies an expected DNS name, Email address or IP address. TLS servers rarely solicit client certificates, and even when they do, they generally don't perform a name check against a reference identifier (expected identity), but rather extract the presented identity after checking the certificate chain. So TLS servers are generally not affected and the severity of the issue is Moderate. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

**CWE:** [CWE-843: Access of Resource Using Incompatible Type \('Type Confusion'\)](https://cwe.mitre.org/data/definitions/843.html)

(<https://cwe.mitre.org/data/definitions/843.html>)

**CVSS Source:** CISA ADP

**CVSS Base score:** 7.5

**CVSS Vector:** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

**CVEID:** [CVE-2024-45310](https://www.cve.org/CVERecord?id=CVE-2024-45310) (https://www.cve.org/CVERecord?id=CVE-2024-45310)

**DESCRIPTION:** runc is a CLI tool for spawning and running containers according to the OCI specification. runc 1.1.13 and earlier, as well as 1.2.0-rc2 and earlier, can be tricked into creating empty files or directories in arbitrary locations in the host filesystem by sharing a volume between two containers and exploiting a race with `os.MkdirAll`. While this could be used to create empty files, existing files would not be truncated. An attacker must have the ability to start containers using some kind of custom volume configuration. Containers using user namespaces are still affected, but the scope of places an attacker can create inodes can be significantly reduced. Sufficiently strict LSM policies (SELinux/Apparmor) can also in principle block this attack -- we suspect the industry standard SELinux policy may restrict this attack's scope but the exact scope of protection hasn't been analysed. This is exploitable using runc directly as well as through Docker and Kubernetes. The issue is fixed in runc v1.1.14 and v1.2.0-rc3. Some workarounds are available. Using user namespaces restricts this attack fairly significantly such that the attacker can only create inodes in directories that the remapped root user/group has write access to. Unless the root user is remapped to an actual user on the host (such as with rootless containers that don't use `/etc/sub[ug]id`), this in practice means that an attacker would only be able to create inodes in world-writable directories. A strict enough SELinux or AppArmor policy could in principle also restrict the scope if a specific label is applied to the runc runtime, though neither the extent to which the standard existing policies block this attack nor what exact policies are needed to sufficiently restrict this attack have been thoroughly tested.

**CWE:** [CWE-61: UNIX Symbolic Link \(Symlink\) Following](https://cwe.mitre.org/data/definitions/61.html) (https://cwe.mitre.org/data/definitions/61.html)

**CVSS Source:** CVE.org

**CVSS Base score:** 3.6

**CVSS Vector:** (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N)

**CVEID:** [CVE-2024-55565](https://www.cve.org/CVERecord?id=CVE-2024-55565) (https://www.cve.org/CVERecord?id=CVE-2024-55565)

**DESCRIPTION:** nanoid (aka Nano ID) before 5.0.9 mishandles non-integer values. 3.3.8 is also a fixed version.

**CWE:** [CWE-835: Loop with Unreachable Exit Condition \('Infinite Loop'\)](https://cwe.mitre.org/data/definitions/835.html) (https://cwe.mitre.org/data/definitions/835.html)

**CVSS Source:** CISA ADP

**CVSS Base score:** 4.3

**CVSS Vector:** (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

**CVEID:** [CVE-2024-6345](https://www.cve.org/CVERecord?id=CVE-2024-6345) (https://www.cve.org/CVERecord?id=CVE-2024-6345)

**DESCRIPTION:** pypa/setuptools could allow a remote attacker to execute arbitrary code on the system, caused by an error in the package\_index module. By persuading a victim to click a specially crafted URL, an attacker could exploit this vulnerability using its download functions to inject and execute arbitrary code on the system.

**CWE:** [CWE-94: Improper Control of Generation of Code \('Code Injection'\)](https://cwe.mitre.org/data/definitions/94.html)

(https://cwe.mitre.org/data/definitions/94.html)

**CVSS Source:** IBM X-Force

**CVSS Base score:** 8.8

**CVSS Vector:** (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

**CVEID:** [CVE-2024-55912](https://www.cve.org/CVERecord?id=CVE-2024-55912) (https://www.cve.org/CVERecord?id=CVE-2024-55912)

**DESCRIPTION:** IBM Concert Software uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.

**CWE:** [CWE-327: Use of a Broken or Risky Cryptographic Algorithm](https://cwe.mitre.org/data/definitions/327.html) (https://cwe.mitre.org/data/definitions/327.html)

**CVSS Source:** IBM

**CVSS Base score:** 5.9

**CVSS Vector:** (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

**CVEID:** [CVE-2024-51744](https://www.cve.org/CVERecord?id=CVE-2024-51744) (https://www.cve.org/CVERecord?id=CVE-2024-51744)

**DESCRIPTION:** golang-jwt jwt-go could allow a remote attacker to obtain sensitive information, caused by improper error handling in ParseWithClaims. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

**CWE:** [CWE-755: Improper Handling of Exceptional Conditions](https://cwe.mitre.org/data/definitions/755.html) (https://cwe.mitre.org/data/definitions/755.html)

**CVSS Source:** IBM X-Force

**CVSS Base score:** 3.1

**CVSS Vector:** (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)

**CVEID:** [CVE-2024-49766](https://www.cve.org/CVERecord?id=CVE-2024-49766) (https://www.cve.org/CVERecord?id=CVE-2024-49766)

**DESCRIPTION:** Werkzeug is a Web Server Gateway Interface web application library. On Python < 3.11 on Windows, os.path.isabs() does not catch UNC paths like //server/share. Werkzeug's safe\_join() relies on this check, and so can produce a path that is not safe, potentially allowing unintended access to data. Applications using Python >= 3.11, or not using Windows, are not vulnerable. Werkzeug version 3.0.6 contains a patch.

**CWE:** [CWE-22: Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](https://cwe.mitre.org/data/definitions/22.html) (https://cwe.mitre.org/data/definitions/22.html)

**CVSS Source:** security-advisories@github.com

**CVSS Base score:** 6.3

**CVSS Vector:**

(CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X)

**CVEID:** [CVE-2024-49767](https://www.cve.org/CVERecord?id=CVE-2024-49767) (https://www.cve.org/CVERecord?id=CVE-2024-49767)

**DESCRIPTION:** Werkzeug is a Web Server Gateway Interface web application library. Applications using `werkzeug.formparser.MultiPartParser` corresponding to a version of Werkzeug prior to 3.0.6 to parse `multipart/form-data` requests (e.g. all flask applications) are vulnerable to a relatively simple but effective resource exhaustion (denial of service) attack. A specifically crafted form submission request can cause the parser to allocate and block 3 to 8 times the upload size in main memory. There is no upper limit; a single upload at 1 Gbit/s can exhaust 32 GB of RAM in less than 60 seconds. Werkzeug version 3.0.6 fixes this issue.

**CWE:** [CWE-400: Uncontrolled Resource Consumption](https://cwe.mitre.org/data/definitions/400.html) (<https://cwe.mitre.org/data/definitions/400.html>)

**CVSS Source:** CVE.org

**CVSS Base score:** 6.9

**CVSS Vector:** (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)

**CVEID:** [CVE-2024-55913](https://www.cve.org/CVERecord?id=CVE-2024-55913) (<https://www.cve.org/CVERecord?id=CVE-2024-55913>)

**DESCRIPTION:** IBM Concert Software could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (`/../`) to view arbitrary files on the system.

**CWE:** [CWE-22: Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](https://cwe.mitre.org/data/definitions/22.html)

(<https://cwe.mitre.org/data/definitions/22.html>)

**CVSS Source:** IBM

**CVSS Base score:** 5.3

**CVSS Vector:** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

**CVEID:** [CVE-2024-55910](https://www.cve.org/CVERecord?id=CVE-2024-55910) (<https://www.cve.org/CVERecord?id=CVE-2024-55910>)

**DESCRIPTION:** IBM Concert Software is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.

**CWE:** [CWE-918: Server-Side Request Forgery \(SSRF\)](https://cwe.mitre.org/data/definitions/918.html) (<https://cwe.mitre.org/data/definitions/918.html>)

**CVSS Source:** IBM

**CVSS Base score:** 6.5

**CVSS Vector:** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

**CVEID:** [CVE-2023-39325](https://www.cve.org/CVERecord?id=CVE-2023-39325) (<https://www.cve.org/CVERecord?id=CVE-2023-39325>)

**DESCRIPTION:** Golang Go is vulnerable to a denial of service, caused by an uncontrolled resource consumption flaw in the net/http and x/net/http2 packages. By sending specially crafted requests using HTTP/2 client, a remote attacker could exploit this vulnerability to cause a denial of service condition.

**CWE:** [CWE-770: Allocation of Resources Without Limits or Throttling](https://cwe.mitre.org/data/definitions/770.html) (<https://cwe.mitre.org/data/definitions/770.html>)

**CVSS Source:** IBM X-Force

**CVSS Base score:** 7.5

**CVSS Vector:** (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

**CVEID:** [CVE-2023-39326](https://www.cve.org/CVERecord?id=CVE-2023-39326) (<https://www.cve.org/CVERecord?id=CVE-2023-39326>)

**DESCRIPTION:** Golang Go could allow a remote attacker to obtain sensitive information, caused by a flaw in the net/http package. By sending a specially crafted HTTP request, an attacker could exploit this vulnerability to read many more bytes from the network than are in the body, and use this information to launch further attacks against the affected system.

**CVSS Source:** IBM X-Force

**CVSS Base score:** 5.3

**CVSS Vector:** (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

**CVEID:** [CVE-2023-45284](https://www.cve.org/CVERecord?id=CVE-2023-45284) (https://www.cve.org/CVERecord?id=CVE-2023-45284)

**DESCRIPTION:** Golang Go could provide weaker than expected security, caused by the failure to correctly detect reserved device names in some cases by the IsLocal function in the filepath package. An attacker could exploit this vulnerability to report "COM1", and reserved names "COM" and "LPT" followed by superscript 1, 2, or 3 as local.

**CVSS Source:** IBM X-Force

**CVSS Base score:** 5.3

**CVSS Vector:** (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

**CVEID:** [CVE-2024-45338](https://www.cve.org/CVERecord?id=CVE-2024-45338) (https://www.cve.org/CVERecord?id=CVE-2024-45338)

**DESCRIPTION:** An attacker can craft an input to the Parse functions that would be processed non-linearly with respect to its length, resulting in extremely slow parsing. This could cause a denial of service.

**CWE:** [CWE-1333: Inefficient Regular Expression Complexity](https://cwe.mitre.org/data/definitions/1333.html) (https://cwe.mitre.org/data/definitions/1333.html)

**CVSS Source:** CISA ADP

**CVSS Base score:** 5.3

**CVSS Vector:** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

**IBM X-Force ID:** 191433

**DESCRIPTION:** Intel Running Average Power Limit (RAPL) Interface for multiple Processors could allow a local authenticated attacker to obtain sensitive information, caused by improper access control in the Linux kernel driver. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

**CWE:** [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](https://cwe.mitre.org/data/definitions/200.html)

(https://cwe.mitre.org/data/definitions/200.html)

**CVSS Source:** IBM X-Force

**CVSS Base score:** 5.6

**CVSS Vector:** (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)

## Affected Products and Versions

Affected Product(s)	Version(s)
IBM Concert Software	1.0.0-1.0.5

## Remediation/Fixes

IBM strongly recommends addressing the vulnerability now by upgrading to IBM Concert Software 1.1.0


Download IBM Concert Software 1.1.0 from Container software library section of IBM Entitled Registry ([ICR](https://myibm.ibm.com/products-services/containerlibrary) (https://myibm.ibm.com/products-services/containerlibrary)) and follow [installation instructions](#)

(<https://www.ibm.com/docs/en/concert?topic=installing-preparing-run-installs-from-private-container-registry>) depending on the type of deployment.

## Workarounds and Mitigations

None

## Get Notified about Future Security Bulletins

 Subscribe to [My Notifications](#) (<https://www.ibm.com/support/pages/node/718119>) to be notified of important product support alerts like this.

## References

[Complete CVSS v3 Guide](#) 

[On-line Calculator v3](#) 

## Related Information

[IBM Secure Engineering Web Portal](#) (<http://www.ibm.com/security/secure-engineering/bulletins.html>)

[IBM Product Security Incident Response Blog](#) (<http://www.ibm.com/blogs/psirt>)

## Acknowledgement

## Change History

30 Apr 2025: Initial Publication

\*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

## Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions"

referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

---

## Document Information

**More support for:**  
IBM Concert Software

**Software version:**  
1.0

**Operating system(s):**  
Linux

**Document number:**  
7232169

**Modified date:**  
30 April 2025