



Security Bulletin: SHA-1 cipher suites detected in older versions of SPSS Statistics (CVE-2024-31896)

Security Bulletin

Summary

The Statistics server supports SHA-1 cipher suites. SHA-1 was officially deprecated by NIST in 2011, but many applications still rely on it. Up until 2017, only theoretical attacks have been known against SHA-1, which is why many applications still rely on it. Recently, a practical attack was introduced by CWI Amsterdam and Google Research teams. For more details refer: <http://shattered.io/static/shattered.pdf>

Vulnerability Details

CVEID: [CVE-2024-31896](https://www.cve.org/CVERecord?id=CVE-2024-31896) (<https://www.cve.org/CVERecord?id=CVE-2024-31896>)

DESCRIPTION: IBM SPSS Statistics 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 X-Force

CVSS Base score: 5.9

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

Affected Products and Versions

| Affected Product(s) | Version(s) |
|---------------------|------------|
| SPSS Statistics | 26.0 |
| SPSS Statistics | 27.0.1 |
| SPSS Statistics | 28.0.1 |
| SPSS Statistics | 29.0.2 |

Remediation/Fixes

The SHA-1 cypher suite was previously present in SPSS Statistics 26.0, SPSS Statistics 27.0.1, SPSS Statistics 28.0.1, SPSS Statistics 29.0.2. The issue has been fixed in all but version 26, for which a free upgrade is available.

Statistics Server 29.0.2.0, IF006 - [29.0.2.0-IM-S29STATS-WIN-LINUX-IF006](#)

(https://www.ibm.com/support/fixcentral/swg/selectFixes?fixids=29.0.2.0-IM-S29STATS-WIN-LINUX-IF006&product=ibm%2FInformation%20Management%2FSPSS%20Statistics&source=dbluesearch&mhsrc=ibmsearch_a&mhq=29%26period%3B0%26period%3B2%26period%3B0-IM-S29STATS-WIN-LINUX-IF006&function=fixId&parent=SPSS)

Statistics Server 28.0.1.1 IF011 - [28.0.1.1-IM-S27STAT-ALL-IF011](#)

(https://www.ibm.com/support/fixcentral/swg/selectFixes?fixids=28.0.1.1-IM-S27STAT-ALL-IF011&product=ibm%2FInformation%20Management%2FSPSS%20Statistics&source=dbluesearch&mhsrc=ibmsearch_a&mhq=28%26period%3B0%26period%3B1%26period%3B1-IM-S27STAT-ALL-IF011&function=fixId&parent=SPSS)

Statistics Server 27.0.1.0 IF030 (LINUX platforms only) - [27.0.1.0-IM-S27STATS-LINUX-IF030](#)

(https://www.ibm.com/support/fixcentral/swg/selectFixes?fixids=27.0.1.0-IM-S27STATS-LINUX-IF030&product=ibm%2FInformation%20Management%2FSPSS%20Statistics&source=dbluesearch&mhsrc=ibmsearch_a&mhq=27%26period%3B0%26period%3B1%26period%3B0-IM-S27STATS-LINUX-IF030&function=fixId&parent=SPSS)

Customers using IBM SPSS Statistics version 26 who do not have S&S support and who are concerned about this issue can be provided with an upgrade to version 27 at no additional cost.


- 1 Navigate to <https://www.ibm.com/support/pages/node/6333515> (<https://www.ibm.com/support/pages/node/6333515>)
- 2 Choose type "Other licensing requests"
- 3 Enter in your own words that you have IBM SPSS Statistics version 26 and need to download version 27 due to Security Bulletin SB0021841

A support case will then be created to provide authorized users of version 26 with an upgrade to version 27.

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

-  Subscribe to [My Notifications](https://www.ibm.com/support/pages/node/718119) (<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](#) 

Reference:

<https://en.wikipedia.org/wiki/SHA-1> (<https://en.wikipedia.org/wiki/SHA-1>)

<https://www.ssl.com/article/is-sha1-considered-weak-ssl> (<https://www.ssl.com/article/is-sha1-considered-weak-ssl>)

Related Information

None

Acknowledgement

Change History

25 Mar 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 SPSS Statistics](https://www.ibm.com/mysupport/s/topic/0TO500000001yjtGAA) (<https://www.ibm.com/mysupport/s/topic/0TO500000001yjtGAA>)

Software version:

26, 27.0.1, 28.0.1, 29.0.2

Operating system(s):

Mac OS, Windows, Linux, Linux on IBM Z Systems

Document number:

7228971

Modified date:

25 March 2025