



CVE-2014-0852

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0852
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-16 04:39:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	IBM WebSphere DataPower SOA appliances through 4.0.2.15, 5.x through 5.0.0.17, 6.0.0.x through 6.0.0.9, and 6.0.1.x through 6.0.1.9 are vulnerable to a side channel timing attack that can be used to decrypt sensitive information. The vulnerability is caused by a flaw in the SSL/TLS implementation that allows an attacker to observe the timing of the decryption process. This can be used to deduce the plaintext of the encrypted data. The vulnerability is present in the SSL/TLS implementation of the WebSphere DataPower SOA appliances. The vulnerability is present in the SSL/TLS implementation of the WebSphere DataPower SOA appliances. The vulnerability is present in the SSL/TLS implementation of the WebSphere DataPower SOA appliances.

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	IBM	WebSphere DataPower Soa Appliance	-	All	All	All
Hardware	IBM	WebSphere DataPower Soa Appliance	-	All	All	All
Operating System	IBM	WebSphere DataPower Soa Appliance Firmware	5.0.0	All	All	All
Operating System	IBM	WebSphere DataPower Soa Appliance Firmware	6.0.0	All	All	All
Operating System	IBM	WebSphere DataPower Soa Appliance Firmware	6.0.1	All	All	All
Operating System	IBM	WebSphere DataPower Soa Appliance Firmware	5.0.0	All	All	All
Operating System	IBM	WebSphere DataPower Soa Appliance Firmware	6.0.0	All	All	All
Operating System	IBM	WebSphere DataPower Soa Appliance Firmware	6.0.1	All	All	All
Operating System	IBM	WebSphere DataPower Soa Appliance Firmware	All	All	All	All

References

Reference	Source
Security Bulletin: SSL/TLS side channel timing vulnerability on WebSphere DataPower (CVE-2014-0852)	CO
IBM X-Force Exchange	XI
IT01111: SECURITY CVE-2014-0852 SSL/TLS SIDE CHANNEL DECRYPTION VULNERABILITY	AI
Security Advisory SA60112 - IBM WebSphere DataPower SOA Appliances SSL/TLS Timing Information Disclosure Weakness - Secunia	SI
CVE Program record	C'

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)