



CVE-2012-0193

Published on: 01/19/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:23 PM UTC

CVE-2012-0193

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Websphere Application Server](#) from [Ibm](#) contain the following vulnerability:

IBM WebSphere Application Server (WAS) 6.0 through 6.0.2.43, 6.1 before 6.1.0.43, 7.0 before 7.0.0.23, and 8.0 before 8.0.0.3 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted

parameters.

CVE-2012-0193 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM notice: The page you requested cannot be displayed

[www-01.ibm.com](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[AIXAPAR PM53930](#)

PM53930: Collisions in HashTable May Cause DoS Vulnerability

[Patch](#)

[Vendor Advisory](#)

[www-01.ibm.com](#)

[text/html](#)

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg24031821](#)

Potential security vulnerability when using Web based applications on IBM WebSphere Application Server due to Java HashTable implementation vulnerability (PM53930/PM57565)

[Patch](#)

[Vendor Advisory](#)

[www-01.ibm.com](#)

[text/html](#)

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21577532](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Application Server	6.0.0.0	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.0	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.12	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.0	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.15	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.19	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.21	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.23	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.25	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.27	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.29	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.31	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.33	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.35	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.37	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.4	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.42	All	All	All

[illegible]

[illegible]

[illegible]

Application	ibm	Websphere Application Server	8.0.0.0	All	All	All
Application	ibm	Websphere Application Server	8.0.0.1	All	All	All
Application	ibm	Websphere Application Server	8.0.0.2	All	All	All
cpe:2.3:a:ibm:websphere_application_server:6.0.0.0:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.2:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.3:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.1.0:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.1.11:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.1.12:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.0:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.1:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.11:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.13:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.15:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.17:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.19:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.2:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.21:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.23:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.25:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.27:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.29:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.3:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.31:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.33:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.35:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.37:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.4:*:*:*:*:*.*						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.43:*:*:*:*:*.*						

cpe:2.3:a:ibm:websphere_application_server:6.0.2.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.6:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.8:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.9:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.13:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.14:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.33:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.35:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.37:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.39:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.41:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*****:

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.15:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.17:::*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.19:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.21:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:8.0.0.0:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:8.0.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:8.0.0.2:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.0.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.0.2:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.0.3:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.1.11:::*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.1.12:::*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.0:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.11:::*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.13:*:*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.15:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.17:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.19:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.2:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.21:::*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.0.2.23:*:*:*:*:*.*
```

cpe:2.3:a:ibm:websphere_application_server:6.0.2.25:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.27:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.29:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.3:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.31:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.33:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.35:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.37:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.4:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.43:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.5:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.6:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.7:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.8:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.9:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.13:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.14:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.33:*****:

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](#).

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