



CVE-2018-1992

Published on: 03/21/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

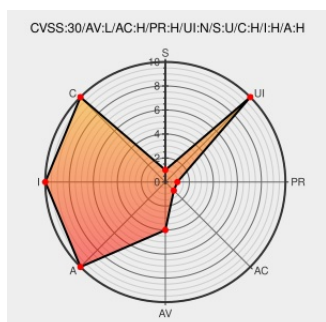
CVE-2018-1992

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Power System Ac922 8335-gtg](#) from [Ibm](#) contain the following vulnerability:

The IBM Power 9 OP910, OP920, and FW910 boot firmware's bootloader is responsible for loading and validating the initial boot firmware image that drives the rest of the system's hardware initialization. The bootloader firmware contains a buffer overflow vulnerability such that, if an attacker were able to replace the initial

boot firmware image with a very carefully crafted and sufficiently large, malicious replacement, it could cause the bootloader, during the load of that image, to overwrite its own instruction memory and circumvent secure boot protections, install trojans, etc. IBM X-Force ID: 154345.

CVE-2018-1992 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [IBM](#) - **Power 9 Systems** version **FW910**

Affected Vendor/Software: [IBM](#) - **Power 9 Systems** version **OP910**

Affected Vendor/Software: [IBM](#) - **Power 9 Systems** version **OP920**

CVSS3 Score: **6.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact				
COMPLETE	COMPLETE	COMPLETE				
CVE References						
Description	Tags	Link				
Security Bulletin: This Power System update is being released to address CVE 2018-1992	Vendor Advisory www.ibm.com text/html	 CONFIRM www.ibm.com/support/docview.wss?uid=ibm10868992				
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	 XF ibm-power9-cve20181992-code-exec (154345)				
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
Hardware 	ibm	Power System Ac922 8335-gtg	-	All	All	All
Operating System	ibm	Power System Ac922 8335-gtg Firmware	All	All	All	All
Hardware 	ibm	Power System Ac922 8335-gth	-	All	All	All
Operating System	ibm	Power System Ac922 8335-gth Firmware	All	All	All	All
Hardware 	ibm	Power System Ac922 8335-gtx	-	All	All	All
Operating System	ibm	Power System Ac922 8335-gtx Firmware	All	All	All	All
Hardware 	ibm	Power System Ac922 8335-gtg	-	All	All	All
Hardware 	ibm	Power System Ac922 8335-gtg	-	All	All	All
Operating System	ibm	Power System Ac922 8335-gtg Firmware	All	All	All	All
Operating System	ibm	Power System Ac922 8335-gtg Firmware	All	All	All	All
Hardware 	ibm	Power System Ac922 8335-gth	-	All	All	All
Hardware 	ibm	Power System Ac922 8335-gth	-	All	All	All
Operating System	ibm	Power System Ac922 8335-gth Firmware	All	All	All	All
Operating System	ibm	Power System Ac922 8335-gth Firmware	All	All	All	All

System							
Hardware  	lbn	Power System Ac922 8335-gtx	-	All	All	All	
Hardware  	lbn	Power System Ac922 8335-gtx	-	All	All	All	
Operating System	lbn	Power System Ac922 8335-gtx Firmware	All	All	All	All	
Operating System	lbn	Power System Ac922 8335-gtx Firmware	All	All	All	All	
Hardware  	lbn	Power System H922 9223-22h	-	All	All	All	
Operating System	lbn	Power System H922 9223-22h Firmware	All	All	All	All	
Hardware  	lbn	Power System H922 9223-22h	-	All	All	All	
Hardware  	lbn	Power System H922 9223-22h	-	All	All	All	
Operating System	lbn	Power System H922 9223-22h Firmware	All	All	All	All	
Operating System	lbn	Power System H922 9223-22h Firmware	All	All	All	All	
Hardware  	lbn	Power System H924 9223-42h	-	All	All	All	
Operating System	lbn	Power System H924 9223-42h Firmware	All	All	All	All	
Hardware  	lbn	Power System H924 9223-42h	-	All	All	All	
Hardware  	lbn	Power System H924 9223-42h	-	All	All	All	
Operating System	lbn	Power System H924 9223-42h Firmware	All	All	All	All	
Operating System	lbn	Power System H924 9223-42h Firmware	All	All	All	All	
Hardware  	lbn	Power System L922 9008-22l	-	All	All	All	
Operating System	lbn	Power System L922 9008-22l Firmware	All	All	All	All	
Hardware  	lbn	Power System L922 9008-22l	-	All	All	All	
Hardware  	lbn	Power System L922 9008-22l	-	All	All	All	
Operating System	lbn	Power System L922 9008-22l Firmware	All	All	All	All	
Operating System	lbn	Power System L922 9008-22l Firmware	All	All	All	All	
Hardware  	lbn	Power System Lc921 9006-12p	-	All	All	All	
Operating System	lbn	Power System Lc921 9006-12p Firmware	All	All	All	All	
Hardware  	lbn	Power System Lc921 9006-12p	-	All	All	All	
Hardware  	lbn	Power System Lc921 9006-12p	-	All	All	All	

Operating System	lbm	Power System Lc921 9006-12p Firmware	All	All	All	All
Operating System	lbm	Power System Lc921 9006-12p Firmware	All	All	All	All
Hardware  	lbm	Power System Lc922 9006-22p	-	All	All	All
Operating System	lbm	Power System Lc922 9006-22p Firmware	All	All	All	All
Hardware  	lbm	Power System Lc922 9006-22p	-	All	All	All
Hardware  	lbm	Power System Lc922 9006-22p	-	All	All	All
Operating System	lbm	Power System Lc922 9006-22p Firmware	All	All	All	All
Operating System	lbm	Power System Lc922 9006-22p Firmware	All	All	All	All
Hardware  	lbm	Power System S914 9009-41a	-	All	All	All
Operating System	lbm	Power System S914 9009-41a Firmware	All	All	All	All
Hardware  	lbm	Power System S914 9009-41a	-	All	All	All
Hardware  	lbm	Power System S914 9009-41a	-	All	All	All
Operating System	lbm	Power System S914 9009-41a Firmware	All	All	All	All
Operating System	lbm	Power System S914 9009-41a Firmware	All	All	All	All
Hardware  	lbm	Power System S922 9009-22a	-	All	All	All
Operating System	lbm	Power System S922 9009-22a Firmware	All	All	All	All
Hardware  	lbm	Power System S922 9009-22a	-	All	All	All
Hardware  	lbm	Power System S922 9009-22a	-	All	All	All
Operating System	lbm	Power System S922 9009-22a Firmware	All	All	All	All
Operating System	lbm	Power System S922 9009-22a Firmware	All	All	All	All
Hardware  	lbm	Power System S924 9009-42a	-	All	All	All
Operating System	lbm	Power System S924 9009-42a Firmware	All	All	All	All
Hardware  	lbm	Power System S924 9009-42a	-	All	All	All
Hardware  	lbm	Power System S924 9009-42a	-	All	All	All
Operating System	lbm	Power System S924 9009-42a Firmware	All	All	All	All
Operating System	lbm	Power System S924 9009-42a Firmware	All	All	All	All

```
cpe:2.3:h:ibm:power_system_ac922_(8335-gtg):-:*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power_system_ac922_(8335-gtg)_firmware:*.:.:.:.:.:
```

```
cpe:2.3:h:ibm:power_system_ac922_(8335-gth):-:*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power_system_ac922_(8335-gth)_firmware:*:*:*:*:*:
```

```
cpe:2.3:h:ibm:power_system_ac922_(8335-gtx):-:*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power_system_ac922_(8335-gtx)_firmware:*.*.*.*.*.*
```

```
cpe:2.3:h:ibm:power_system_ac922_\\(8335-gtg\\):-:*:*:*:*:*:
```

```
cpe:2.3:h:ibm:power_system_ac922_\\(8335-gtg\\):-:*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power_system_ac922_(8335-gtg)\_firmware:*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power_system_ac922_\\(8335-gtg\\)_firmware:*.:.:.:.:.:
```

```
cpe:2.3:h:ibm:power_system_ac922_(8335-gth\):-:*:*:*:*:*:
```

```
cpe:2.3:h:ibm:power_system_ac922_(8335-gth\):-:*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power system ac922 \(8335-qth\) firmware:*.***.***.***.
```

```
cpe:2.3:o:ibm:power_system_ac922_(8335-gth)_firmware:*:*:*:*:*:
```

```
cpe:2.3:h:ibm:power_system_ac922_\\(8335-gtx\\):-:*:*:*:*:*:
```

```
cpe:2.3:h:ibm:power_system_ac922_\(8335-gtx\):::*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power_system_ac922_(8335-gtx)_firmware:*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:ibm:power_system_ac922_\\(8335-gtx\\)_firmware:*.***.***.***
```

```
cpe:2.3:h:ibm:power_system_h922_(9223-22h):-:*:*:*:*:*:
```

```
cpe:2.3:o:ibm:power_system_h922_(9223-22h)_firmware:*.:.:.:.:.:
```

```
cpe:2.3:h:ibm:power_system_h922_(9223-22h):-:*:*:*:*:*:
```

```
cpe:2.3:h:ibm:power system h922 \((9223-22h\)):-:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:o:ibm:power_system_h922_(9223-22h)_firmware:*.***.***.***:
```

```
cpe:2.3:o:ibm:power_system_h922_(9223-22h)_firmware:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:ibm:power_system_h924_(9223-42h):-:*:*:*:*:*:*
```

```
cpe:2.3:o:ibm:power_system_h924_(9223-42h)_firmware:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:ibm:power_system_h924_\\(9223-42h\\):-:*:*:*:*:*:
```

```
cpe:2.3:h:ibm:power system h924 \((9223-42h)\):-:*~::~
```

```
cpe:2.3:o:ibm:power_system_h924_(9223-42h)_firmware:*:*:*:*:*:
```

cpe:2.3:o:ibm:power_system_h924_(9223-42h\)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_l922_(9008-22l):-:*.*****:
cpe:2.3:o:ibm:power_system_l922_(9008-22l)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_l922_(9008-22l):-:*.*****:
cpe:2.3:h:ibm:power_system_l922_(9008-22l):-:*.*****:
cpe:2.3:o:ibm:power_system_l922_(9008-22l)_firmware:*.*****:
cpe:2.3:o:ibm:power_system_l922_(9008-22l)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_lc921_(9006-12p):-:*.*****:
cpe:2.3:o:ibm:power_system_lc921_(9006-12p)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_lc921_(9006-12p):-:*.*****:
cpe:2.3:h:ibm:power_system_lc921_(9006-12p):-:*.*****:
cpe:2.3:o:ibm:power_system_lc921_(9006-12p)_firmware:*.*****:
cpe:2.3:o:ibm:power_system_lc921_(9006-12p)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_lc922_(9006-22p):-:*.*****:
cpe:2.3:o:ibm:power_system_lc922_(9006-22p)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_lc922_(9006-22p):-:*.*****:
cpe:2.3:h:ibm:power_system_lc922_(9006-22p):-:*.*****:
cpe:2.3:o:ibm:power_system_lc922_(9006-22p)_firmware:*.*****:
cpe:2.3:o:ibm:power_system_lc922_(9006-22p)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_s914_(9009-41a):-:*.*****:
cpe:2.3:o:ibm:power_system_s914_(9009-41a)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_s914_(9009-41a):-:*.*****:
cpe:2.3:h:ibm:power_system_s914_(9009-41a):-:*.*****:
cpe:2.3:o:ibm:power_system_s914_(9009-41a)_firmware:*.*****:
cpe:2.3:o:ibm:power_system_s914_(9009-41a)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_s922_(9009-22a):-:*.*****:
cpe:2.3:o:ibm:power_system_s922_(9009-22a)_firmware:*.*****:
cpe:2.3:h:ibm:power_system_s922_(9009-22a):-:*.*****:

cpe:2.3:h:ibm:power_system_s922_(9009-22a):-:*****:
cpe:2.3:o:ibm:power_system_s922_(9009-22a)_firmware:*****:
cpe:2.3:o:ibm:power_system_s922_(9009-22a)_firmware:*****:
cpe:2.3:h:ibm:power_system_s924_(9009-42a):-:*****:
cpe:2.3:o:ibm:power_system_s924_(9009-42a)_firmware:*****:
cpe:2.3:h:ibm:power_system_s924_(9009-42a):-:*****:
cpe:2.3:h:ibm:power_system_s924_(9009-42a):-:*****:
cpe:2.3:o:ibm:power_system_s924_(9009-42a)_firmware:*****:
cpe:2.3:o:ibm:power_system_s924_(9009-42a)_firmware:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)