



CVE-2019-13927

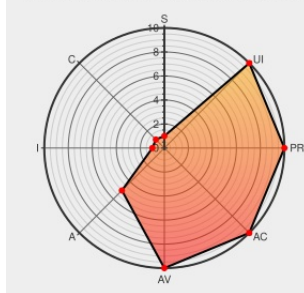
Published on: 12/12/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-13927

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L



Certain versions of [Pxa30-w0](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Desigo PX automation controllers PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D with Desigo PX Web modules PXA40-W0, PXA40-W1, PXA40-W2 (All firmware versions < V6.00.320), Desigo PX automation controllers PXC00-U, PXC64-U, PXC128-U with Desigo PX Web modules PXA30-W0,

PXA30-W1, PXA30-W2 (All firmware versions < V6.00.320), Desigo PX automation controllers PXC22.1-E.D, PXC36-E.D, PXC36.1-E.D with activated web server (All firmware versions < V6.00.320). The device contains a vulnerability that could allow an attacker to cause a denial of service condition on the device's web server by sending a specially crafted HTTP message to the web server port (tcp/80). The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device's web service. While the device itself stays operational, the web server responds with HTTP status code 404 (Not found) to any further request. A reboot is required to recover the web interface. At the time of advisory publication no public exploitation of this security vulnerability was known.

CVE-2019-13927 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [S](#) Siemens AG - Desigo PX automation controllers PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D with Desigo PX Web modules PXA40-W0, PXA40-W1, PXA40-W2 version All firmware versions < V6.00.320

Affected Vendor/Software: [S](#) Siemens AG - Desigo PX automation controllers PXC00-U, PXC64-U, PXC128-U with Desigo PX Web modules PXA30-W0, PXA30-W1, PXA30-W2 version All firmware versions < V6.00.320

Affected Vendor/Software: [S](#) Siemens AG - Desigo PX automation controllers PXC22.1-E.D, PXC36-E.D, PXC36.1-E.D with activated web server version All firmware versions < V6.00.320

CVSS3 Score: **5.3 - MEDIUM**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

NETWORK		LOW		NONE		NONE	
Scope		Confidentiality Impact		Integrity Impact		Availability Impact	
UNCHANGED		NONE		NONE		LOW	
CVSS2 Score: 5 - MEDIUM							
Access Vector		Access Complexity		Authentication			
NETWORK		LOW		NONE			
Confidentiality Impact		Integrity Impact		Availability Impact			
NONE		NONE		PARTIAL			
CVE References							
Description		Tags		Link			
		Vendor Advisory cert-portal.siemens.com application/pdf		 MISC cert-portal.siemens.com/productcert/pdf/ssa-898181.pdf			
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 	Siemens	Pxa30-w0	-	All	All	All	
Hardware 	Siemens	Pxa30-w0	-	All	All	All	
Operating System	Siemens	Pxa30-w0 Firmware	All	All	All	All	
Operating System	Siemens	Pxa30-w0 Firmware	All	All	All	All	
Hardware 	Siemens	Pxa30-w1	-	All	All	All	
Hardware 	Siemens	Pxa30-w1	-	All	All	All	
Operating System	Siemens	Pxa30-w1 Firmware	All	All	All	All	
Operating System	Siemens	Pxa30-w1 Firmware	All	All	All	All	
Hardware 	Siemens	Pxa30-w2	-	All	All	All	
Hardware 	Siemens	Pxa30-w2	-	All	All	All	

Operating System	Siemens	Pxa30-w2 Firmware	All	All	All	All
Operating System	Siemens	Pxa30-w2 Firmware	All	All	All	All
Hardware 	Siemens	Pxa40-w0	-	All	All	All
Hardware 	Siemens	Pxa40-w0	-	All	All	All
Operating System	Siemens	Pxa40-w0 Firmware	All	All	All	All
Operating System	Siemens	Pxa40-w0 Firmware	All	All	All	All
Hardware 	Siemens	Pxa40-w1	-	All	All	All
Hardware 	Siemens	Pxa40-w1	-	All	All	All
Operating System	Siemens	Pxa40-w1 Firmware	All	All	All	All
Operating System	Siemens	Pxa40-w1 Firmware	All	All	All	All
Hardware 	Siemens	Pxa40-w2	-	All	All	All
Hardware 	Siemens	Pxa40-w2	-	All	All	All
Operating System	Siemens	Pxa40-w2 Firmware	All	All	All	All
Operating System	Siemens	Pxa40-w2 Firmware	All	All	All	All
Hardware 	Siemens	Pxc00-e.d	-	All	All	All
Hardware 	Siemens	Pxc00-e.d	-	All	All	All
Operating System	Siemens	Pxc00-e.d Firmware	All	All	All	All
Operating System	Siemens	Pxc00-e.d Firmware	All	All	All	All
Hardware 	Siemens	Pxc00-u	-	All	All	All
Hardware 	Siemens	Pxc00-u	-	All	All	All
Operating System	Siemens	Pxc00-u Firmware	All	All	All	All
Operating System	Siemens	Pxc00-u Firmware	All	All	All	All
Hardware 	Siemens	Pxc100-e.d	-	All	All	All
Hardware 	Siemens	Pxc100-e.d	-	All	All	All
Operating System	Siemens	Pxc100-e.d Firmware	All	All	All	All
Operating System	Siemens	Pxc100-e.d Firmware	All	All	All	All
Hardware 	Siemens	Pxc100-u	-	All	All	All

Hardware  	Siemens	Pxc128-u	-	All	All	All
Hardware  	Siemens	Pxc128-u	-	All	All	All
Operating System	Siemens	Pxc128-u Firmware	All	All	All	All
Operating System	Siemens	Pxc128-u Firmware	All	All	All	All
Hardware  	Siemens	Pxc200-e.d	-	All	All	All
Hardware  	Siemens	Pxc200-e.d	-	All	All	All
Operating System	Siemens	Pxc200-e.d Firmware	All	All	All	All
Operating System	Siemens	Pxc200-e.d Firmware	All	All	All	All
Hardware  	Siemens	Pxc22.1-e.d	-	All	All	All
Hardware  	Siemens	Pxc22.1-e.d	-	All	All	All
Operating System	Siemens	Pxc22.1-e.d Firmware	All	All	All	All
Operating System	Siemens	Pxc22.1-e.d Firmware	All	All	All	All
Hardware  	Siemens	Pxc36-e.d	-	All	All	All
Hardware  	Siemens	Pxc36-e.d	-	All	All	All
Operating System	Siemens	Pxc36-e.d Firmware	All	All	All	All
Operating System	Siemens	Pxc36-e.d Firmware	All	All	All	All
Hardware  	Siemens	Pxc36.1-e.d	-	All	All	All
Hardware  	Siemens	Pxc36.1-e.d	-	All	All	All
Operating System	Siemens	Pxc36.1-e.d Firmware	All	All	All	All
Operating System	Siemens	Pxc36.1-e.d Firmware	All	All	All	All
Hardware  	Siemens	Pxc50-e.d	-	All	All	All
Hardware  	Siemens	Pxc50-e.d	-	All	All	All
Operating System	Siemens	Pxc50-e.d Firmware	All	All	All	All
Operating System	Siemens	Pxc50-e.d Firmware	All	All	All	All
Hardware  	Siemens	Pxc64-u	-	All	All	All
Hardware  	Siemens	Pxc64-u	-	All	All	All
Operating System	Siemens	Pxc64-u Firmware	All	All	All	All

Operating System	Siemens	Pxc64-u Firmware	All	All	All	All
cpe:2.3:h:siemens:pxa30-w0:-:*:*:*:*:*:						
cpe:2.3:h:siemens:pxa30-w0:-:*:*:*:*:*:						
cpe:2.3:o:siemens:pxa30-w0_firmware:*:*:*:*:*:						
cpe:2.3:o:siemens:pxa30-w0_firmware:*:*:*:*:*:						
cpe:2.3:h:siemens:pxa30-w1:-:*:*:*:*:*:						
cpe:2.3:h:siemens:pxa30-w1:-:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa30-w1_firmware:*:*:*:*:*:						
cpe:2.3:o:siemens:pxa30-w1_firmware:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa30-w2:-:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa30-w2:-:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa30-w2_firmware:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa30-w2_firmware:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa40-w0:-:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa40-w0:-:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa40-w0_firmware:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa40-w0_firmware:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa40-w1:-:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa40-w1:-:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa40-w1_firmware:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa40-w1_firmware:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa40-w2:-:*:*:*:*::~:						
cpe:2.3:h:siemens:pxa40-w2:-:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa40-w2_firmware:*:*:*:*::~:						
cpe:2.3:o:siemens:pxa40-w2_firmware:*:*:*:*::~:						
cpe:2.3:h:siemens:pxc00-e.d:-:*:*:*:*::~:						
cpe:2.3:h:siemens:pxc00-e.d:-:*:*:*:*::~:						
cpe:2.3:o:siemens:pxc00-e.d_firmware:*:*:*:*::~:						

```
cpe:2.3:o:siemens:pxc00-e.d_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc00-u:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc00-u:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc00-u_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc00-u_firmware:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc100-e.d:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc100-e.d:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc100-e.d firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc100-e.d_firmware:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc128-u:-:*:*:*:*:*:*:
```

cpe:2.3:h:siemens:pxc128-u:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:pxc128-u_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc128-u_firmware:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc200-e.d:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc200-e.d:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc200-e.d_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc200-e.d_firmware:*:*:*:*:*:*.*
```

cpe:2.3:h:siemens:pxc22.1-e.d:-:*:*:*:*:*:

```
cpe:2.3:h:siemens:pxc22.1-e.d:-:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc22.1-e.d_firmware:*.:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc22.1-e.d_firmware:*.:*:*:*:*:*.*
```

cpe:2.3:h:siemens:pxc36-e.d:-:*:*:*:*:*:*:

cpe:2.3:h:siemens:pxc36-e.d:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:pxc36-e.d_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc36-e.d_firmware:*:*:*:*:*:*:*:
```

cpe:2.3:h:siemens:pxc36.1-e.d:-:*:*:*:*:*:*:

cpe:2.3:h:siemens:pxc36.1-e.d:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:pxc36.1-e.d firmware:*:*:*:*:*:*:*:
```

```
opc'2 3:0:siemens:nxc26 1 0 d firmware:*.*.*.*.*.*.*.*.

```

```

Cpe.2.5.0.Siemens.px000.f-e.u_firmware. . . . .

```

cpe:2.3:h:siemens:pxc50-e.d:-:*:*:*:*:*:*:

cpe:2.3:h:siemens:pxc50-e.d:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:pxc50-e.d firmware:*.***.***.***.
```

```
cpe:2.3:o:siemens:pxc50-e.d firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc64-u:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:pxc64-u:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:pxc64-u firmware:*.~*~*~*~*~*~*~*~*~*
```

```
cpe:2.3:o:siemens:pxc64-u firmware:*.~*~*~*~*~*~*~*~*~*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status status.cve.report