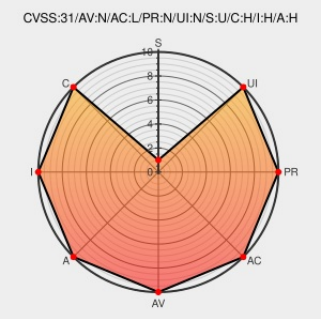
CVE-2020-5616

Published on: 08/03/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5616

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Calendar01 from Calendar01 Project contain the following vulnerability:

[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors.

CVE-2020-5616 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **PHP Factory** - **[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01]** version **[Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
JVN#73169744: Multiple vulnerabilities in multiple PHP Factory products	Third Party Advisory jvn.jp text/xml	MISC jvn.jp/en/jp/JVN73169744/index.html
【Telop01】PHPテロップ・ニュースティッカー・ヘッドラインCMSフリー（無料）版（スマホ対応）｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/telop/01.php
【PKOBO-vote01】PHP投票・アンケートシステム（連続、多重投票防止付き）CMS フリー（無料）版｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/vote/01.php
【Calendar01】PHP営業日カレンダー・スケジュールカレンダーCMS フリー（無料）版｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/calendar/01.php
PHP営業日・スケジュールカレンダー（テキスト入力付）CMS　フリー（無料）版｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/calendar/02.php
PHPリンク集ページCMS フリー（無料）版｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/link/01.php
PHP写真ギャラリー（フォトアルバム）CMS　フリー（無料）｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/gallery/01.php
受付上限設定付き　PHP予約・応募フォーム連動 営業日カレンダー フリー（無料）版｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/calendar_form/01.php
【PKOBO-News01】PHP新着情報・お知らせ・ニュースCMSプログラム　フリー（無料）版｜PHP工房	Product Third Party Advisory www.php-factory.net text/html	MISC www.php-factory.net/news/pkobo-news01.php

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Calendar01 Project	Calendar01	1.0.0	All	All	All

Application	Calendar01 Project	Calendar01	1.0.0	All	All	All
Application	Calendar02 Project	Calendar02	1.0.0	All	All	All
Application	Calendar02 Project	Calendar02	1.0.0	All	All	All
Application	Calendarform01 Project	Calendarform01	All	All	All	All
Application	Gallery01 Project	Gallery01	All	All	All	All
Application	Link01 Project	Link01	1.0.0	All	All	All
Application	Link01 Project	Link01	1.0.0	All	All	All
Application	Pkobo-news01 Project	Pkobo-news01	All	All	All	All
Application	Pkobo-vote01 Project	Pkobo-vote01	All	All	All	All
Application	Telop01 Project	Telop01	1.0.0	All	All	All
Application	Telop01 Project	Telop01	1.0.0	All	All	All

cpe:2.3:a:calendar01_project:calendar01:1.0.0:*:*:*:free:*:*:*:

cpe:2.3:a:calendar01_project:calendar01:1.0.0:*:*:*:free:*:*:*:

cpe:2.3:a:calendar02_project:calendar02:1.0.0:*:*:*:free:*:*:*:

cpe:2.3:a:calendar02_project:calendar02:1.0.0:*:*:*:free:*:*:*:

cpe:2.3:a:calendarform01_project:calendarform01:*:*:*:*:free:*:*:*:

cpe:2.3:a:gallery01_project:gallery01:*:*:*:*:free:*:*:*:

cpe:2.3:a:link01_project:link01:1.0.0:*:*:*:free:*:*:*:

cpe:2.3:a:link01_project:link01:1.0.0:*:*:*:free:*:*:*:

cpe:2.3:a:pkobo-news01_project:pkobo-news01:*:*:*:*:free:*:*:*:

cpe:2.3:a:pkobo-vote01_project:pkobo-vote01:*:*:*:*:free:*:*:*:

cpe:2.3:a:telop01_project:telop01:1.0.0:*:*:*:free:*:*:*:

cpe:2.3:a:telop01_project:telop01:1.0.0:*:*:*:free:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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