

Alerta de seguridad cibernética	9VSA20-00284-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2020
Última revisión	17 de agosto de 2020

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de vBulletin referente a vulnerabilidad de ejecución de código remoto que afecta a su software de generación de foro. El presente informe incluye la respectiva medida de mitigación.

## Vulnerabilidad

CVE-2020-7373

## CVE-2020-7373

Vulnerabilidad de tipo ejecución de código remoto sin autenticación permite a un atacante ejecutar código PHP arbitrario dentro del contexto del servidor de aplicaciones (cuenta no-root) mediante el envío de peticiones HTTP especialmente diseñadas.

La prueba de concepto explota un error lógico en la funcionalidad de renderización de plantilla (template rendering functionality), módulo que renderiza a la plantilla "widget\_tabbedcontainer\_tab\_panel" mientras que provee del argumento "widget\_php", lo cual provoca que la plantilla mencionada cargue al argumento mencionado, evadiendo filtros diseñados originalmente para subsanar al CVE-2019-16759.

### Productos Afectados

VBulletin Connect versiones 5.6.2, 5.6.1 y 5.6.0. Versiones anteriores también son consideradas vulnerables.

### Mitigaciones

Descargar y aplicar parches de seguridad disponibles para las versiones 5.6.2, 5.6.1 y 5.6.0. Versiones anteriores deben actualizar urgentemente a la versión 5.6.2 para evitar ser vulnerables.

### Enlaces

[https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements\\_aa/4445227-vbulletin-5-6-0-5-6-1-5-6-2-security-patch](https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4445227-vbulletin-5-6-0-5-6-1-5-6-2-security-patch)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7373>