infomicro

INFORME DE VULNERABILIDADES

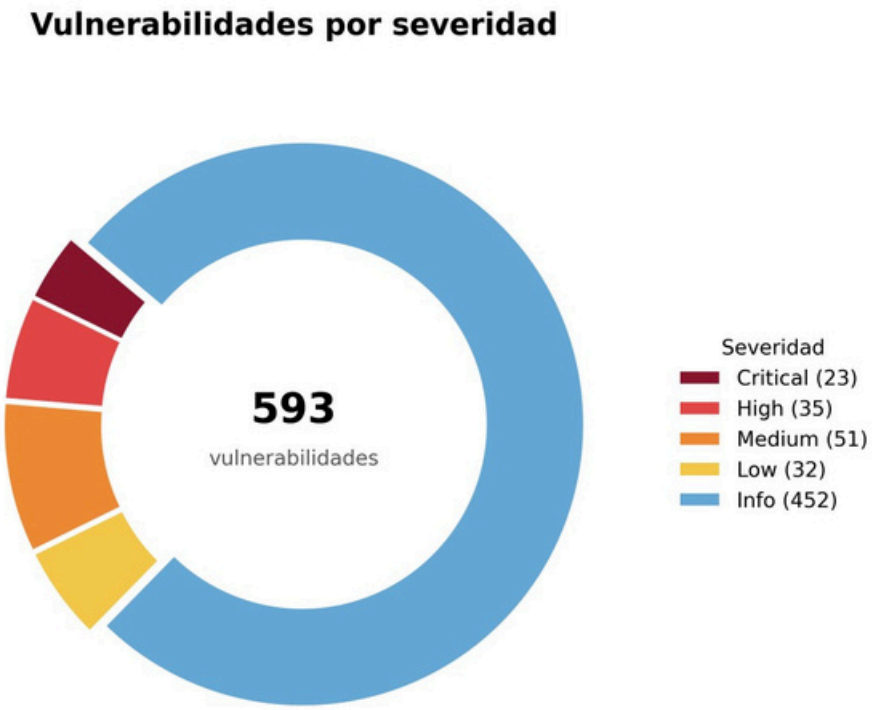
infomicro

ÍNDICE

RESUMEN GLOBAL DE VULNERABILIDADES

VULNERABILIDADES ENCONTRADAS

Total: 593
Informativas: 452
Bajas: 32 **Medias:** 42 **Altas:** 30
Críticas: 23



A continuación, se detallan las vulnerabilidades encontradas, comenzando por las clasificadas como críticas, seguido del resto de niveles de severidad.

RESUMEN GLOBAL DE VULNERABILIDADES

DETALLE TÉCNICO - VM VIRTUAL

Total: 287
Informativas: 181
Bajas: 15 **Medias:** 51 **Altas:** 35
Críticas: 19

A continuación, se detallan las vulnerabilidades encontradas, comenzando por las clasificadas como críticas, seguido del resto de niveles de severidad.

DETALLADO DE VULNERABILIDADES

KB5066586:Windows10version1809 / Windows Server 2019 Security Update (October 2025)

KB5066586:Windows10version1809 / Windows Server 2019 Security Update (October 2025)

CVSS Score:9.9 VPR Score:9.4 La ausenciadelaactualización de seguridad KB5066586 en sistemas como Windows 10 versión1809yWindows Server 2019 deja...

Oracle Java SE Multiple Vulnerabilities (October 2025 CPU)

CVSS Score: 7.5 VPR Score: 9.2 El compromiso de Oracle Java SE y sus componentes puede permitir a atacantes no autenticados, con acceso a la red mediante múltiples protocolos, explotar diversas vulnerabilidades para tomar el control del sistema. Estas fallas...

WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

CVSS Score: 8.8 VPR Score: 9.0 La falta de configuración adecuada en ciertas claves del registro puede dejar al sistema expuesto a ataques remotos. Un atacante...

Security Update for Microsoft .NET Core (July 2024)

CVSS Score: 7.3 VPR Score: 8.4 El impacto de esta vulnerabilidad radica en la posibilidad de elevar privilegios en aplicaciones desarrolladas con .NET, .NET Framework y Visual Studio. Esto permite...

DETALLADO DE VULNERABILIDADES

KB5066586:Windows10version1809 / Windows Server 2019 Security Update (October 2025)

KB5066586:Windows10version1809 / Windows Server 2019 Security Update (October 2025)

CVSS Score:9.9 VPR Score:9.4 La ausenciadelaactualización de seguridad KB5066586 en sistemas como Windows 10 versión1809yWindows Server 2019 deja...

Oracle Java SE Multiple Vulnerabilities (October 2025 CPU)

CVSS Score: 7.5 VPR Score: 9.2 El compromiso de Oracle Java SE y sus componentes puede permitir a atacantes no autenticados, con acceso a la red mediante múltiples protocolos, explotar diversas vulnerabilidades para tomar el control del sistema. Estas fallas...

WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

CVSS Score: 8.8 VPR Score: 9.0 La falta de configuración adecuada en ciertas claves del registro puede dejar al sistema expuesto a ataques remotos. Un atacante...

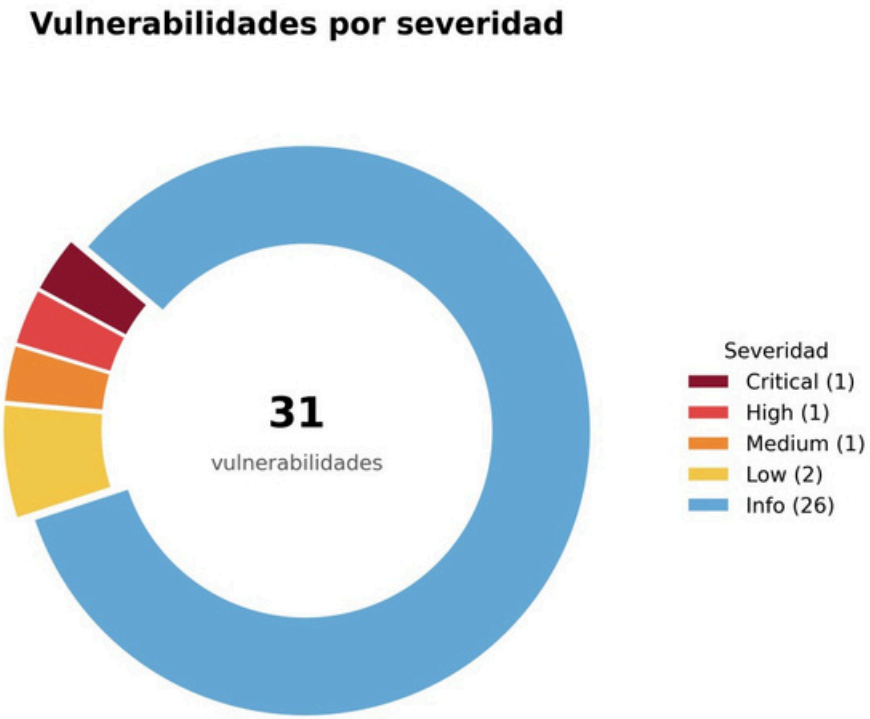
Security Update for Microsoft .NET Core (July 2024)

CVSS Score: 7.3 VPR Score: 8.4 El impacto de esta vulnerabilidad radica en la posibilidad de elevar privilegios en aplicaciones desarrolladas con .NET, .NET Framework y Visual Studio. Esto permite...

VULNERABILIDADES ENCONTRADAS

DETALLE TÉCNICO - SERVIDOR FÍSICO

Total: 31
Informativas: 26
Bajas: 2 **Medias:** 1 **Altas:** 1
Críticas: 1



A continuación, se detallan las vulnerabilidades encontradas, comenzando por las clasificadas como críticas, seguido del resto de niveles de severidad.

DETALLADO DE VULNERABILIDADES

XXX Multiple Vulnerabilities (XXX-202X-000X)

CVSS Score: 9.3
VPR Score: 9.2
Explotar estas vulnerabilidades en XXX podría permitir a un atacante que ya tiene privilegios administrativos en una máquina virtual ejecutar...

SSL Self-Signed Certificate

CVSS Score: 6.5
VPR Score: -
El uso de un certificado SSL autofirmado debilita gravemente la seguridad de la conexión, ya que no se puede validar la identidad...

XXX Multiple Vulenerabilities (XXX-202x-000)

CVSS Score: 6.8
VPR Score: 6.7
El uso de versiones vulnerables de XXX puede permitir a un atacante ejecutar un ataque de denegación de servicio...

CVSS Score: 6.8
VPR Score: 6.7
El uso de versiones vulnerables de XXX puede permitir a un atacante ejecutar un ataque de denegación de servicio...
La falta de confianza en el certificado X.509 del servidor puede comprometer...

VULNERABILIDADES ENCONTRADAS

DETALLE TÉCNICO - DISPOSITIVO NAS

Total: 51
Informativas: 44
Bajas: 6 **Medias:** 1 **Altas:** 0
Críticas: 0

A continuación, se detallan las vulnerabilidades encontradas, comenzando por las clasificadas como críticas, seguido del resto de niveles de severidad.

DETALLADO DE VULNERABILIDADES

OpenSSH < 10.1 / 10.1p1 Multiple Vulnerabilities

CVSS Score: 3.6
VPR Score: 4.0
El uso de versiones anteriores a 10.1 de OpenSSH presenta múltiples vulnerabilidades que podrían ser explotadas por un atacante. La inclusión de caracteres de control...

ICMP Timestamp Request Remote Date Disclosure

CVSS Score: 2.1*
VPR Score: 2.2
La exposición del tiempo del sistema mediante solicitudes de ICMP puede facilitar a un atacante remoto no autenticado eludir protocolos de autenticación basados en el tiempo.

SSL Certificate Cannot Be Trusted

CVSS Score: 6.5
VPR Score: -
El hecho de que un certificado X.509 no pueda ser confiable pone en riesgo la autenticidad de la comunicación entre el servidor y los usuarios. Cuando la cadena de confianza se rompe, esto puede facilitar ataques de tipo man-in-the-middle, comprometendo la integridad de los datos transmitidos.

SMB Signing not required

CVSS Score: 5.3
VPR Score: -
La falta de requerimiento de firmas en el servidor SMB permite a un atacante remoto no autenticado llevar a cabo...

VULNERABILIDADES ENCONTRADAS

DETALLE TÉCNICO - DISPOSITIVO DE RED

Total: 44
Informativas: 41
Bajas: 3 **Medias:** 0 **Altas:** 0
Críticas: 0

A continuación, se detallan las vulnerabilidades encontradas, comenzando por las clasificadas como críticas, seguido del resto de niveles de severidad.

DETALLADO DE VULNERABILIDADES

SSL Certificate Cannot Be Trusted

CVSS Score: 6.5
VPR Score: -
El hecho de que el certificado X.509 del servidor no pueda ser confiable afecta gravemente la seguridad de las comunicaciones. Esto puede ocurrir...

SSL Self-Signed Certificate

CVSS Score: 6.5
VPR Score: -
El uso de un certificado SSL autofirmado para un servicio plantea serios riesgos de seguridad, ya que carece...

TLS Version 1.1 Deprecated Protocol

CVSS Score: 6.5
VPR Score: -
El uso de TLS 1.1 presenta un grave riesgo de seguridad debido a su falta de soporte para los conjuntos de cifrados...

PLAN DE MITIGACIÓN GLOBAL

Alta prioridad (Corto plazo)
DISPOSITIVO DE RED

Media prioridad (Medio plazo)

Baja prioridad (Largo plazo)