

# Trend Micro Worry-Free Business Security Unauthenticated Remote File Deletion

High

[← View More Research Advisories](#)

## Synopsis

### Unauthenticated Path Traversal

Trend Micro's Worry-Free Business Security (WFBS) version 10.0, build 2228 and below are vulnerable to an unauthenticated path traversal allowing for remote file deletion. The specific flaw exists within the ErrorRemoveLogTempFile function in cgiLog.exe when handling of the BinaryDataBlock parameter provided to the /officescan/cgi/cgiLog.exe endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in a file deletion operation. An unauthenticated remote attacker can exploit the vulnerability to delete arbitrary files using the CURL command provided in the PoC section of this advisory. The file deletion operation runs under the security context of the user account running the WFBS web server. WFBS can install and use Apache as its web server, which runs under the Local System account by default.

## Solution

Update to Trend Micro Worry-Free Business Security 10 SP1 Patch 2260.

## Proof of Concept

```
curl -ki -d 'event=19&uid=12345678-1234-1234-1234-123456789012AAAA&BinaryDataBlock=../../../../../../../../<path_of_file_to_be_deleted>' 'https://<wfbs_host>:4343/officescan/cgi/cgiLog.exe'
```

## Additional References

<https://success.trendmicro.com/solution/000281948>

## Disclosure Timeline

08/17/2020 - Tenable reports vulnerability to TrendMicro  
08/17/2020 - Trend Micro acknowledges receipt.  
08/31/2020 - Tenable follows up with Trend Micro asking for updates.  
09/14/2020 - Tenable follows up asking for updates  
09/28/2020 - Tenable again follows up asking for updates  
09/28/2020 - Trend Micro responds that it is still being looked into  
10/13/2020 - Tenable follows up for any new updates  
10/13/2020 - Trend Micro says developers still working on a patch  
10/27/2020 - Tenable follows up for any new updates  
10/27/2020 - Trend Micro says developers still working on a patch  
11/09/2020 - Tenable follows up asking for expected patch date and reminding that public disclosure will be next week  
11/12/2020 - Tenable asks Trend Micro for CVE number if they plan on issuing one.  
11/12/2020 - Trend Micro asks for 1 day extension to disclosure in order to a fix JP localized version  
11/16/2020 - Tenable informs that our disclosure policy releases advisories in 90 days with-or-without a patch, and an extension is not possible.

*All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.*

*Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.*

*For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.*

*If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)*

## Risk Information

**CVE ID:** [CVE-2020-28574](#)

**Tenable Advisory ID:** TRA-2020-62

**CVSSv2 Base / Temporal Score:** 9.4

**CVSSv2 Vector:** AV:N/AC:L/Au:N/C:N/I:C/A:C

**Affected Products:** Trend Micro Worry-Free Business Security

**Risk Factor:** High

## Advisory Timeline

11/16/2020 - Advisory published.

11/18/2020 - Added CVE and Solution

[Tenable.io Vulnerability Management](#)

[Tenable.io Web App Scanning](#)

[Tenable.asm External Attack Surface](#)

[Tenable.ad Active Directory](#)

[Tenable.ot Operational Technology](#)

[Tenable.sc Security Center](#)

[Tenable Lumin](#)

[Nessus](#)

[→ View all Products](#)

#### FEATURED SOLUTIONS

[Application Security](#)

[Building Management Systems](#)

[Cloud Security Posture Management](#)

[Compliance](#)

[Exposure Management](#)

[Finance](#)

[Healthcare](#)

[IT/OT](#)

[Ransomware](#)

[State / Local / Education](#)

[US Federal](#)

[Vulnerability Management](#)

[Zero Trust](#)

[→ View all Solutions](#)

#### CUSTOMER RESOURCES

[Resource Library](#)

[Community & Support](#)

[Customer Education](#)

[Tenable Research](#)

[Documentation](#)

[Trust and Assurance](#)

[Nessus Resource Center](#)

[Cyber Exposure Fundamentals](#)

[System Status](#)

#### CONNECTIONS

[Blog](#)

[Contact Us](#)

[Careers](#)

[Investors](#)

[Events](#)

[Media](#)