Analysis Report for: E98EB4AC54913315811B438B09B800B9.exe.vbs

Overall Functionality

This code snippet is not C code; it's a batch script (.bat file) for Windows. It sets a series of environment variables. These variables define various system parameters, paths, and seemingly encoded data. The variables include system information (processor architecture, OS version, paths), user-specific data (user name, temporary directories), and application-specific paths (Java, SQL Server, OneDrive). The presence of `IGCCSVC_DB` which contains a Base64 encoded string, is particularly suspicious. The script doesn't perform any actions beyond setting these environment variables; it doesn't execute any programs or manipulate files.

Function Summaries

There are no functions in a batch script in the same way that there are in C. The script consists solely of `set` commands, which assign values to environment variables.

Control Flow

The control flow is extremely simple and linear. It's a sequence of `set` commands, executed one after another. There are no loops or conditional statements (e.g., `if`, `for`).

Data Structures

There are no explicit data structures used. The data is implicitly stored as strings in environment variables.

Malware Family Suggestion

While the script itself doesn't contain malicious code that directly performs harmful actions (like deleting files or sending data), the setting of numerous environment variables, especially the Base64 encoded string in `IGCCSVC_DB`, strongly suggests it's part of a larger malicious operation. This is characteristic of several malware families, especially those designed for persistence or data exfiltration. The encoded data likely contains configuration information or instructions for subsequent malicious actions by a main program. Given the significant number of system-related environment variables set, it's likely intended to mimic normal system operation while potentially enabling further malicious activity. The most likely malware family would be a **downloader** or **dropper**, designed to fetch or execute a more sophisticated payload. This script would be one component in the infection chain. A static analysis would not be sufficient; dynamic analysis is needed to understand what it does when executed.

Further Analysis Recommendations

1. **Decode the Base64 string:** The value assigned to `IGCCSVC_DB` needs to be decoded to understand its contents. This might reveal URLs, commands, or other clues about the malware's intentions.
2. **Analyze the complete system:** This script is likely only one part of a larger infection. A full system scan with updated antivirus software is crucial to remove any other components.
3. **Reverse engineer any subsequent executables:** If this script launches any other executables, reverse engineering those programs is essential to understand the full extent of the malware's capabilities.
4. **Monitor network traffic:** If the script communicates over a network, monitoring this traffic may reveal communication with command-and-control servers or data exfiltration attempts.

In summary, while this batch script looks innocuous at first glance, its contents strongly indicate it plays a support role in a malware infection, and caution and further analysis are required to determine the malware's exact function.