CIRT.GY Guyana National Computer Incident Response Team

AL2025_09 Microsoft Warns of ViewState Code Injection Attacks Exploiting Exposed ASP.NET Keys (11th February 2025)

Description

Microsoft has issued a warning regarding the misuse of exposed ASP.NET machine keys in ViewState code injection attacks. These attacks leverage static validationKey and decryptionKey values found in publicly available repositories and documentation to execute remote code on compromised IIS web servers. By exploiting these keys, attackers can craft malicious ViewStates, enabling them to deploy malware, execute commands, and establish persistence on targeted systems.

Attack Details

The attack method involves attackers utilizing publicly available ASP.NET machine keys to manipulate ViewState data. ViewState is a mechanism used in ASP.NET Web Forms to maintain the state of web pages across postbacks. When an attacker injects a maliciously crafted ViewState payload into a POST request, the IIS web server decrypts and validates it as legitimate due to the use of valid machine keys. This results in remote code execution (RCE), allowing adversaries to execute arbitrary commands and deploy additional payloads.

In a specific case observed in December 2024, a threat actor used a publicly disclosed machine key to deploy the Godzilla post-exploitation framework on an IIS web server. Godzilla enables command execution and shellcode injection, providing attackers with significant control over compromised environments.

Microsoft has identified over 3,000 publicly disclosed machine keys that can be leveraged in ViewState code injection attacks. Unlike previously known attacks that relied on stolen or compromised keys from underground forums, these keys are accessible through public code repositories, increasing the risk of exploitation.

Remediation

To mitigate the risk of ViewState code injection attacks, Microsoft recommends implementing the following security measures:

Secure Key Management:

- Generate machine keys securely and avoid using default or publicly available keys.
- Encrypt machineKey and connectionStrings elements in the web.config file to prevent unauthorized access.

Upgrade ASP.NET Framework:

- Upgrade applications to ASP.NET 4.8 to take advantage of Antimalware Scan Interface (AMSI) capabilities, which help detect and block malicious activities.

Server Hardening:

- Apply attack surface reduction rules, such as Block Webshell creation for Servers.
- Restrict access to IIS server configuration files and implement strong authentication measures.
- Key Rotation and Remediation:
- Remove or replace exposed ASP.NET keys from web.config using PowerShell or the IIS

Manager Console:

- If successful exploitation is detected, rotating machine keys alone may not be sufficient; a full investigation and possible reinstallation of web-facing servers should be conducted.

By following these best practices, organizations can reduce the risk of ViewState code injection attacks and protect their ASP.NET applications from potential compromise. The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2025, February 10). Microsoft says attackers use exposed ASP.NET keys to deploy malware. Retrieved as BleepingComputer. https://www.bleepingcomputer.com/news/security/microsoft-says-attackers-use-exposed-aspnet-keys-to-deploy-malware/
- Intelligence, M. T. (2025, February 7). Code injection attacks using publicly disclosed ASP.NET machine keys. Retrieved as Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2025/02/06/code-injection-attacks-using-publicly-disclosed-asp-net-machine-keys/