CERT-GH SECURITY ADVISORY

CERT-GH
Ghana Computer Emergency Response Team

Microsoft Silverlight Remote Code Execution Vulnerability

CERT GH REFERENCE #: **CERT-ADV10426022016**
Severity: High
Date Discovered: 13th January 2016

System(s) Affected	All Windows Platforms
Description	Silverlight is a powerful development tool for creating engaging, interactive user experiences for Web and mobile applications. Microsoft Silverlight 5 before 5.1.41212.0 mishandles negative offsets during decoding, which allows remote attackers to execute arbitrary code or cause a denial of service (object-header corruption) via a crafted web site, aka "Silverlight Runtime Remote Code Execution Vulnerability. Microsoft Silverlight is prone to a remote code-execution vulnerability. An attacker can exploit this issue to execute arbitrary code with the privileges of the currently logged-in user. Failed exploit attempts will likely result in a denial-of-service condition.
Impact	The attacker can gain unauthorized access to a vulnerable machine and information may be compromised or stolen. This vulnerability can result in a Denial of Service Attack, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.
Solutions	1. Block external access at the network boundary, unless external parties require service. If global access isn't needed, filter access to the affected computer at the network boundary. Restricting access to only trusted computers and networks might greatly reduce the likelihood of successful exploits. 2. Run all software as a nonprivileged user with minimal access rights. To reduce the impact of latent vulnerabilities, always run nonadministrative software as an unprivileged user with minimal access rights. 3. Do not follow links provided by unknown or untrusted sources. Attackers could

	exploit this vulnerability by enticing a user to visit a malicious website. Do not follow links provided by sources of questionable integrity. 4. Set web browser security to disable the execution of script code or active content. Disable support for script code and active content within a client browser to reduce the chances of a successful exploit. Note that this mitigation tactic might adversely affect legitimate websites that rely on the execution of browser-based script code. 5. Implement multiple redundant layers of security. Since this issue may be leveraged to execute code, we recommend memory-protection schemes, such as nonexecutable stack/heap configurations and randomly mapped memory segments. This tactic may complicate exploits of memory-corruption vulnerabilities. Updates are available. Please see the references or vendor advisory for more information. Visit https://technet.microsoft.com/library/security/ms16-006 for updates
References & Further Information	https://technet.microsoft.com/en-us/library/security/ms16-006.aspx https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0034