OpenSSH - Remote Code Execution

Fellowship Program		
	Title	OpenSSH - Remote Code Execution
	CVE ID	**CVE-2024-6387**
	Description	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.
	Impact	Remote Code Execution
	Affected Version	OpenSSH 8.5p1 to 9.8p1
	Proof Of Concept	Talk to Loc if you have any question

Telerik UI for ASP.NET AJAX - Remote Code Execution

Fellowship Program		
	Title	Telerik UI for ASP.NET AJAX - Remote Code Execution
	CVE ID	**CVE-2019-18935**
	Description	Progress Telerik UI for ASP.NET AJAX through 2019.3.1023 contains a .NET deserialization vulnerability in the RadAsyncUpload function. This is exploitable when the encryption keys are known due to the presence of CVE-2017-11317 or CVE-2017-11357, or other means. Exploitation can result in remote code execution. (As of 2020.1.114, a default setting prevents the exploit. In 2019.3.1023, but not earlier versions, a non-default setting can prevent exploitation.)
	Impact	Execute arbitrary code
	Affected Version	Telerik UI for ASP.NET AJAX through 2019.3.1023
	Proof Of Concept	Talk to Loc if you have any question

Adobe Acrobat Reader - Remote Code Execution

Fellowship Program		
	Title	Adobe Acrobat Reader - Remote Code Execution
	CVE ID	**CVE-2023-21608**
	Description	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
	Impact	Execute arbitrary code
	Affected Version	22.003.20281 (and earlier) and 20.005.30418 (and earlier)
	Proof Of Concept	Talk to Loc if you have any question

IIS HTTP Modules - Remote Code Execution

	Title	IIS HTTP Modules - Remote Code Execution
	CVE ID	**CVE-2023-40044**

Fellowship Program		
	Description	In WS_FTP Server versions prior to 8.7.4 and 8.8.2, a pre-authenticated attacker could leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system.
	Impact	Execute arbitrary code
	Affected Version	IIS HTTP Modules
	Proof Of Concept	Talk to Loc if you have any question

Windows Kernel- Privilege Escalation

Fellowship Program		
	Title	Windows Kernel- Privilege Escalation
	CVE ID	**CVE-2024-21338**
	Description	Windows Kernel Elevation of Privilege Vulnerability
	Impact	Privilege Escalation
	Affected Version	Windows Kernel
	Proof Of Concept	Talk to Loc if you have any question

CraftCMS - Remote Code Execution

Fellowship Program		
	Title	CraftCMS - Remote Code Execution
	CVE ID	**CVE-2025-32432**
	Description	Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.
	Impact	Execute arbitrary code
	Affected Version	from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17
	Proof Of Concept	Talk to Loc if you have any question

Gitlab - Bypass Authentication

	Title	Gitlab - Bypass Authentication
	CVE ID	**CVE-2025-25291**

Fellowship Program		
	Description	ruby-saml provides security assertion markup language (SAML) single sign-on (SSO) for Ruby. An authentication bypass vulnerability was found in ruby-saml prior to versions 1.12.4 and 1.18.0 due to a parser differential. ReXML and Nokogiri parse XML differently; the parsers can generate entirely different document structures from the same XML input. That allows an attacker to be able to execute a Signature Wrapping attack. This issue may lead to authentication bypass. Versions 1.12.4 and 1.18.0 fix the issue.
	Impact	Bypass Authentication
	Affected Version	prior to versions 1.12.4 and 1.18.0
	Proof Of Concept	Talk to Loc if you have any question

Grafana - SSRF

Fellowship Program		
	Title	Grafana - SSRF
	CVE ID	**CVE-2025-4123**
	Description	A cross-site scripting (XSS) vulnerability exists in Grafana caused by combining a client path traversal and open redirect. This allows attackers to redirect users to a website that hosts a frontend plugin that will execute arbitrary JavaScript. This vulnerability does not require editor permissions and if anonymous access is enabled, the XSS will work. If the Grafana Image Renderer plugin is installed, it is possible to exploit the open redirect to achieve a full read SSRF. The default Content-Security-Policy (CSP) in Grafana will block the XSS though the `connect-src` directive.
	Impact	SSRF
	Affected Version	N/A
	Proof Of Concept	Talk to Loc if you have any question