Impactful vulnerabilities detected BloodHound [CVE-2050-001,CVE-2050-002]

Overview

BloodHound is vulnerable to ...
An attacker can use it to ...

The CTI team at Leonardo has detected the following vulnerabilities CVE-2050-001 and CVE-2050-002.

Description

BloodHound is a powerful tool used for visualizing Active Directory environments. Its front-end is built on electron, while the back-end utilizes a Neo4j database. The tool gathers data from a series of data collectors, which are also known as ingestors. These ingestors come in both PowerShell and C# flavors, and they provide information about access control lists (ACLs), users, groups, trust relationships, and other unique AD objects.

BloodHound can be utilized during engagements to identify various attack paths in Active Directory. Both blue and red teams can take advantage of the tool to discover different paths to targets. The following subsections detail the different types of ingestors and how they can be properly utilized. BloodHound is primarily a reconnaissance tool that helps uncover important insights about an organization's Active Directory environment.

On 17 March 2023, 2 vulnerabilities have been disclosed.

Cve-2050-001 is a serious vulnerability that affects certain products offered by Polar. The vulnerability allows for a buffer overrun to be triggered in X.509 certificate verification, specifically in the name constraint checking process. It's important to note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite a failure to construct a path to a trusted issuer. This buffer overflow can have severe consequences, including a crash that could cause a denial of service or potentially lead to remote code execution. The vulnerability has been assigned a cvss score of 7.0, an exploitability score of 8.0, and an impact score of 8.0. The affected Polar products are Star and Coltrane. It's critical to address this vulnerability promptly to prevent potential harm.

Cve-2050-002 is a security vulnerability that affects the Image Hover Effects Css3 WordPress plugin, specifically versions up to and including 4.5. This vulnerability stems from the plugin's failure to properly sanitize and escape some of its settings. As a result, high privilege users, such as admins, may be able to carry out Stored Cross-Site Scripting attacks, even when the unfiltered_html capability is disallowed (for example, in a multisite setup). The vulnerability has been assigned a cvss score of 3.0, an exploitability score of 3.0, and an impact score of 3.0. The affected product is Borges, which is offered by Invictus. It's important to address this vulnerability as soon as possible to prevent potential exploitation and minimize the risk of harm.

The table below includes further details about the vulnerabilities, including the product affected by the security flaw, vendor, CVSSv2 and CVSSv3 score.

ID	CVSSv2	CVSSv3	Vendor	Products	Name
CVE-2050-001	7.0	6.9	Polar	Star and Coltrane	CVE-2050-001
CVE-2050-002	3.0	4.0	Invictus	Borges	CVE-2050-002

Mitigations

Recommended Actions

In line with the CISA guidelines, and following the instructions of the relevant vendor, it is advisable, where possible, to install the latest security updates for products affected by the above vulnerabilities. It is also advisable to prioritize the patching of vulnerabilities affecting services exposed on the Internet and then those with higher CVSS scores.

Appendix 1

CVE-2050-001 CVSS 3.0: 6.9
Vulnerability Description: A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution.
Recommended Mitigations: Privileged Account Management

Detection Methods:

List of detection methods

Vulnerable Configurations:

Polar 3.0 and later

CVSS3					
Base	6.9	Impact	8.0	Exploitability	5.9
Access	Attack Complexity	Attack vector	Privileges Required	Scope	User Interaction
	High	Adjacent	Low	changed	Required
Impact	Confidentiality		Integrity	Availability	
	Low		Low	High	

Source

None

Appendix 2

CVE-2050-002 CVSS 3.0: 4.0

Vulnerability Description:

The Image Hover Effects Css3 WordPress plugin through 4.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).

Recommended Mitigations:

User Training and Restrict Web-Based Content

Detection Methods:

List of detection methods
Vulnerable Configurations: None

CVSS3					
Base	4.0	Impact	3.9	Exploitability	3.9
Access	Attack Complexity	Attack vector	Privileges Required	Scope	User Interaction
	Low	Network	Low	changed	None
Impact	Confidentiality		Integrity	Availability	
	Low		Low	None	

Source

https://access.redhat.com/security/cve/cve-2021-3326