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 tool. The description of BloodHound is: (PenTestPartners) BloodHound is an application used to visualize active directory environments. The front-end is built on electron and the back-end is a Neo4j database, the data leveraged is pulled from a series of data collectors also referred to as ingestors which come in PowerShell and C# flavours.

It can be used on engagements to identify different attack paths in Active Directory (AD), this encompasses access control lists (ACLs), users, groups, trust relationships and unique AD objects. The tool can be leveraged by both blue and red teams to find different paths to targets. The subsections below explain the different and how to properly utilize the different ingestors. The tool type is reconnaissance.

On 17 March 2023, 2 vulnerabilities have been disclosed.

Cve-2050-001 is a vulnerability. The description of the security flaw is: 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. Its cvss score is 7.0. Cve-2050-001 exploitability score is 8.0. Its impact score is 8.0. The vulnerability is present in products offered by Polar. It affects these products Star and Coltrane.

Cve-2050-002 is a vulnerability. The description of the vulnerability is: 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). Its cvss score is 3.0.

Cve-2050-002 exploitability score is 3.0. Its impact score is 3.0. The security flaw is present in products offered by Invictus. The vulnerability affects this product Borges.

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