Code Epic Technologies

Common vulnerabilities and exposure

Surviving technology

cr4sh.m4d0v3r
https://code-epic.github.io

June 2022

1 CVE

The original concept for what would become the CVE List was presented by the co-creators of CVE, The MITRE Corporation's David E. Mann and Steven M. Christey, as a white paper entitled, Towards a Common Enumeration of Vulnerabilities, at the 2nd Workshop on Research with Security Vulnerability Databases on January 21-22, 1999 at Purdue University in West Lafayette, Indiana, USA.

From that original concept, a working group was formed (which would later become the initial 19-member CVE Editorial Board), and the original 321 CVE Records were created. The CVE List was officially launched for the public in September 1999.

Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed information security vulnerabilities and exposures.

CVE was launched in 1999 by the MITRE corporation to identify and categorize vulnerabilities in software and firmware. CVE provides a free dictionary for organizations to improve their cyber security. MITRE is a nonprofit that operates federally funded research and development centers in the United States.

A vulnerability is a weakness that can be exploited in a cyberattack to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow attackers to run code, access system memory, install different types of malware and steal, destroy or modify sensitive data.

An Exposure is a mistake that gives an attacker access to a system or network. Exposures can lead to data breaches, data leaks, and personally identifiable information (PII) being sold on the dark web.

In fact, some of the biggest data breaches were caused by accidental exposures rather than sophisticated cyber attacks.

Standard identifier number

A CVE entry describes a known vulnerability or exposure.

Each CVE entry contains a standard identifier number with status indicator (i.e. "CVE-1999-0067", "CVE-2014-12345", "CVE-2016-7654321"), a brief description and references related vulnerability reports and advisories.

Each CVE ID is formatted as CVE-YYYY-NNNNN. The YYYY portion is the year the CVE ID was assigned or the year the vulnerability was made public.

Unlike vulnerability databases, CVE entries do not include risk, impact fix or other technical information.

Can use CVE to Attack

The short answer is yes but many cybersecurity professionals believe the benefits of CVE outweigh the risks:

1. CVE is restricted to publicly known vulnerabilities and exposures.

2. It improves the shareability of vulnerabilities and exposures within the cybersecurity community.

3. Organizations need to protect themselves and their networks by fixing all potential vulnerabilities and exposures while an attacker only needs to find a single vulnerability and exploit it to gain unauthorized access. This is why a list of known vulnerabilities is so valuable and an important part of network security.

4. The growing agreement for the cybersecurity community to share information is reducing the attack vector of many cyber attacks. This is reflected in widespread acceptance that the CVE Board and CVE Numbering Authorities (CNAs) are key organizations in cybersecurity.

5. As a concrete example, many believe the ransomware WannaCry, which spread through the EternalBlue vulnerability, would have had less impact if the vulnerability was publicly shared.

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. Currently, there are 178,641 CVE Records

The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services. The Exploit Database is a non-profit project that is provided as a public service by Offensive Security.

The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Our aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away.

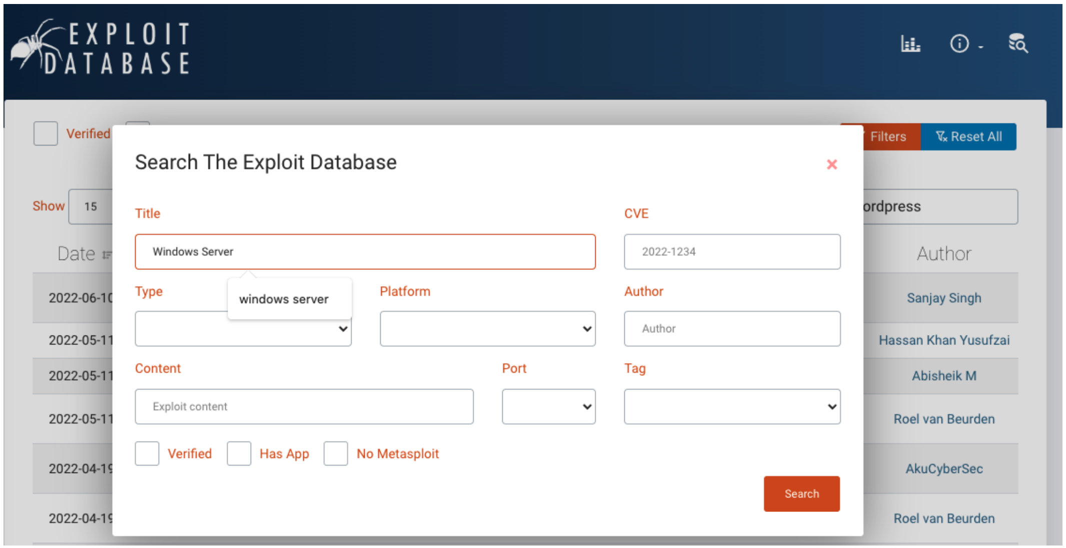
The Google Hacking Database (GHDB) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet. In most cases, this information was never meant to be made public but due to any number of factors this information was linked in a web document that was crawled by a search engine that subsequently followed that link and indexed the sensitive information.

The process known as “Google Hacking” was popularized in 2000 by Johnny Long, a professional hacker, who began cataloging these queries in a database known as the Google Hacking Database. His initial efforts were amplified by countless hours of community member effort, documented in the book Google Hacking For Penetration Testers and popularised by a barrage of media attention and Johnny's talks on the subject such as this early talk recorded at DEFCON 13. Johnny coined the term "Googledork" to refer to "a foolish or inept person as revealed by Google". This was meant to draw attention to the fact that this was not a "Google problem" but rather the result of an often unintentional misconfiguration on the part of a user or a program installed by the user. Over time, the term "dork" became shorthand for a search query that located sensitive information and "dorks" were included with may web application vulnerability releases to show examples of vulnerable web sites.

After nearly a decade of hard work by the community, Johnny turned the GHDB over to Offensive Security in November 2010, and it is now maintained as an extension of the Exploit Database. Today, the GHDB includes searches for other online search engines such as Bing, and other online repositories like GitHub, producing different, yet equally valuable results.

Note

For example, Exploitdb shows us an extensive collection of vulnerabilities, documents and source code in various languages capable of breaking into or exploiting a system failure to gain control of the system. We searched for a vulnerability in the Windows Server system using the searchexploit tool on the website https://www.exploit-db.com/.



Date	Author
2022-06-1	Sanjay Singh
2022-05-11	Hassan Khan Yusufzai
2022-05-11	Abisheik M
2022-05-11	Roel van Beurden
2022-04-1	AkuCyberSec
2022-04-1	Roel van Beurden

Search The Exploit Database

Title: Windows Server

windows server

CVE: 2022-1234

Type:

Platform:

Author: Author

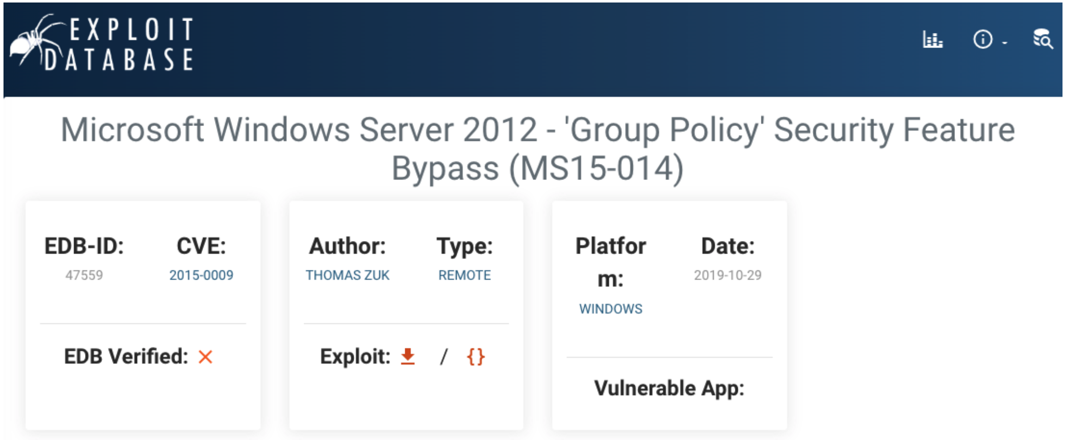
Content: Exploit content

Port:

Tag:

□ Verified □ Has App □ No Metasploit

Search



Microsoft Windows Server 2012 - 'Group Policy' Security Feature Bypass (MS15-014)

EDB-ID: 47559

CVE: 2015-0009

Author: THOMAS ZUK

Type: REMOTE

Platform: WINDOWS

Date: 2019-10-29

EDB Verified: ✗

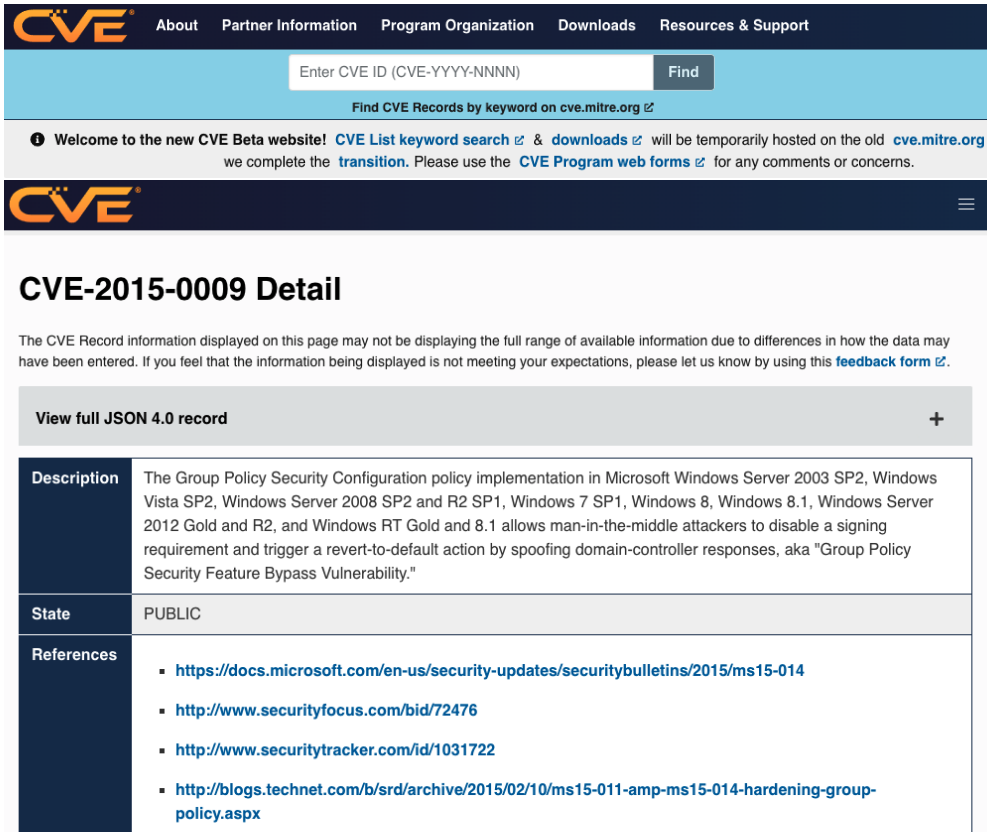
Exploit: / {}

Vulnerable App:

This document is related to a CVE in its description, which allows us to obtain all the details of the vulnerability.

The CVE Record information displayed on this page may not be displaying the full range of available information due to differences in how the data may have been entered.

```
# Exploit Title: Microsoft Windows Server 2012
# 'Group Policy' Security Feature Bypass
# Date: 2019-10-28
# Exploit Author: Thomas Zuk
# Version: Windows Server 2003, Windows Vista
# Windows Server 2008, Windows 7, Windows Server 2008 R2
# Windows 8, Windows Server 2012, Windows RT, Windows 8.1,
# Windows Server 2012 R2, and Windows RT 8.1
# Tested on: Windows 7 , Windows Server 2012
# CVE : CVE-2015-0009
# Type: Remote
# Platform: Windows
```



Welcome to the new CVE Beta website! CVE List keyword search & downloads will be temporarily hosted on the old cve.mitre.org we complete the transition. Please use the CVE Program web forms for any comments or concerns.

CVE-2015-0009 Detail

The CVE Record information displayed on this page may not be displaying the full range of available information due to differences in how the data may have been entered. If you feel that the information being displayed is not meeting your expectations, please let us know by using this feedback form.

View full JSON 4.0 record +

Description	The Group Policy Security Configuration policy implementation in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows man-in-the-middle attackers to disable a signing requirement and trigger a revert-to-default action by spoofing domain-controller responses, aka "Group Policy Security Feature Bypass Vulnerability."
State	PUBLIC
References	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-014 http://www.securityfocus.com/bid/72476 http://www.securitytracker.com/id/1031722 http://blogs.technet.com/b/srd/archive/2015/02/10/ms15-011-amp-ms15-014-hardening-group-policy.aspx

This information presents us with important content when detecting a failure in the system, and a user can with a small source code written in c, python, c++, go or any other language traverse the victim's operating system. visit https://www.exploit-db.com/exploits/47559

OWASP
Open Web Application
Security Project

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

Our Mission

No more insecure software.

As the world's largest non-profit organization concerned with software security, OWASP:

- Supports the building of impactful projects;
- Develops & nurtures communities through events and chapter meetings worldwide; and
- Provides educational publications & resources.
- In order to enable developers to write better software, and security professionals to make the world's software more secure.

OWASP Top Ten

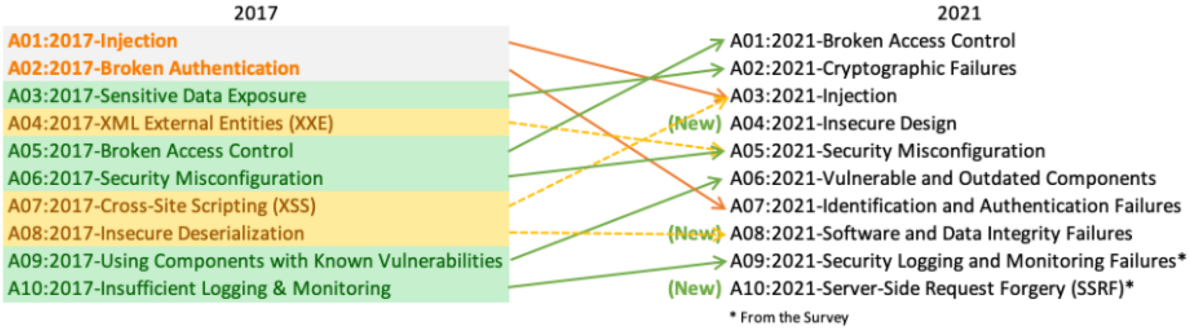
The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

> "Globally recognized by developers as the first step towards more secure coding"

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

- A01:2021-Broken Access Control: 94% of applications were tested for some form of broken access control.
- A02:2021-Cryptographic Failures: Focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- A03:2021-Injection: This category have the second most occurrences in applications. Cross-site Scripting.
- A04:2021-Insecure Design: Is a new category, with a focus on risks related to design flaws the software
- A05:2021-Securty Misconfiguration: With more shifts into highly configurable software, it's not surprising to see this category move up. The

former category for XML External Entities (XXE) is now part of this category.

- A06:2021-Vulnerable and Outdeated Components: It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact are not factored into their scores.

- A07:2021-Identification and Authentication Failures: Is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.

- A08:2021-Software and Data Integrity Failures: Focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity.

- A09:2021-Security Logging and Monitoring Failures: Expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

- A10:2021-Server Side Request Forgery (SSRF): Represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

2 Continues to Grow

In 2016, the CVE Program began actively expanding the number of organizations participating as CVE Numbering Authorities (CNAs). CNA partners are how the CVE List is built. Every CVE Record is added by a CNA. This expansion continues today with more and more organizations from around the world deciding to partner with the CVE Program to become a CNA.

Past Sponsors

1. Defense Information Systems Agency (DISA): Colonel Larry Huffman
2. Department of Energy (DOE): John Przysucha
3. Department of the Treasury: Jim Flyzik
4. General Services Administration: Sallie McDonald
5. Intelligence Community: Bill Dawson
6. Internal Revenue Service (IRS): Len Baptiste
7. MITRE Corporation: Pete Tasker
8. National Aeronautics and Space Administration (NASA): Dave Nelson
9. National Information Assurance Partnership (NIAP): Ron Ross
10. National Infrastructure Protection Center (NIPC): Bob Gerber
11. National Institute of Standards and Technology (NIST): Tim Grance
12. National Security Agency (NSA): Tony Sager
13. U.S. Air Force: Matt Mleziva

OWASP

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.