David Murillo Santiago
Dr. Pugh
IS-3513
22 September 2023

Common Vulnerabilities and Exposures

CVE-2017-9417

CVE-2017-9417 classifies a vulnerability that affects a wide range of Android and iOS devices. Through the vulnerability identified in CVE-2017-9417, devices are susceptible to Broadpwn exploits. Broadpwn targets Broadcom BCM43xx chips which could be found in a wide range of devices, ranging from Apple, to HTC, LG, Nexus, and Samsung devices. In the case of CVE-2017-9417, Broadpwn was reported to allow hackers to remotely exploit a device's Wi-Fi chip to execute arbitrary code. One of the factors contributing to the widespread impact of Broadpwn is as a result of third-party manufacturing. Because OS makers frequently use third-party companies to create chipsets, they do not always know the complete scope of vulnerabilities that go along with their hardware. CVE-2017-9417 is an urgent issue as, if it's exploited successfully, it grants hackers complete control to an effected system. Even in the absence of user activity, the vulnerability continues to pose a threat, demonstrating the severity of the issue and its urgency for resolution. The nature of the vulnerability is particularly urgent because of the helplessness from the user's perspective. There is almost nothing that could be done by the user to mitigate the risk. The only recommendations are to keep their device's software up to date and turn off the device's Wi-Fi feature. Therefore, Broadpwn is a critical issue which must be addressed by operating system developers.

CVE-2023-4185

CVE-2023-4185 classifies a vulnerability that affects hospital management systems. Specifically, this vulnerability was found in SourceCodester Online Hospital Management System 1.0. CVE-2023-4185 represents an SQL injection in the patientlogin.php file, allowing hackers to manipulate the login ID and password with malicious input, which could lead to unauthorized access to sensitive data stored within the system's database. SQL injections are vulnerabilities which occur when web applications fail to adequately validate user input data. Hackers exploit this vulnerability by adding extra commands to the typical requests that systems use, enabling them to carry out attacks. CVE-2023-4185 raises significant security concerns, particularly in applications that handle sensitive healthcare data. HIPAA establishes strict standards for safeguarding patient medical information, with the consequences of a security breach affecting both the individual patient and the organization itself. In the healthcare industry, where confidentiality of patient data is paramount, vulnerabilities like CVE-2023-4185 are severe and demonstrate the necessity of robust security measures to ensure the integrity of sensitive information.

CVE-2019-0708

CVE-2017-0708, also known as BlueKeep, is an infamous vulnerability that poses a threat to Windows-based systems. Windows devices running on Windows 2000, Windows Server 2008 R2, and Windows 7, were susceptible to the CVE-2017-0708 vulnerability. BlueKeep operates by exploiting a weakness in the Remote Desktop Protocol (RDP), which connects a user to a remote server. Before establishing a connection, the protocol undergoes processing by the Remote Desktop Services (RDS), facilitating remote desktop access for users. By sending specially crafted RDS requests, attackers can trigger a buffer overflow, allowing them to execute arbitrary code. BlueKeep is a dangerous vulnerability because it can affect a wide range of Windows machines, and it can be exploited remotely without requiring user interaction.

References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9417

https://resources.infosecinstitute.com/topics/vulnerabilities/broadpwn-wi-fi-vulnerability-detect-mitigate/

https://www.cve.org/CVERecord?id=CVE-2017-9417

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-9417

https://seclists.org/bugtraq/2019/May/30

https://portswigger.net/web-security/sql-injection

https://github.com/Yusoyea/VulList/blob/main/Hospital%20Management%20System%20patientlogin.php%20has%20Sqlinjection.pdf

https://vuldb.com/?id.236220

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4185

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-windows-en

https://cert-portal.siemens.com/productcert/pdf/ssa-166360.pdf