High-Risk Vulnerabilities 2010-2020

Ranking the Worst of the Worst

We took a data-based review of the top vulnerabilities from the past decade to offer you the top vulnerability or vulnerabilities for each of the past 10 years.

This assessment is based on Kenna Security's data science-based calculation of the risk posed by any given CVE to narrow down the worst of the worst vulns—those that earned a Kenna Risk Score of 100 (out of 100). From that list of 171 vulnerabilities, we then picked the most memorable for each year.

KENNA
Security

2010

Stuxnet

Although it occurred just outside of the scope of this project, we would be remiss if we didn't mention CVE-2010-2772 aka Stuxnet. This vulnerability poses very little risk on its own due to the relative rarity of the devices impacted and difficulty to exploit them. However, pairing this vuln with nation-state motivations and a highly targeted mission, and you have all the makings of a Tom Clancy novel.

2011

HP Printer Vulns

Columbia University researchers find RCE vulnerabilities in HP Printers (CVE-2011-2404, CVE-2011-4786) that can potentially be used to produce some fiery results.

2012

VUPEN

Microsoft had 10 vulns that rated a perfect 100 in 2012. VUPEN had some fun demonstrating browser 0-days including one of Microsoft's top 10—an Internet Explorer RCE (CVE-2012-1876). For its efforts, VUPEN took homesome trophies during Pwn2Own at CanSecWest 2012.

2013

MS Office 0-Day

Microsoft warns its users about an Office 0-Day (CVE-2013-3906) that enables RCE via an TIFF image embedded in an office document. This vuln was being exploited in the wild so users needed to be cautious until the patch was available in the following weeks' patch Tuesday.

2014

Shellshock, Sandworm, and Heartbleed - oh, my!

- Shellshock aka Bashdoor (CVE-2014-6271) hits the scene.
- With Dune hitting theaters (and HBO Max) in 2021, only fitting to call out the emergence of the Sandworm (CVE-2014-4114) malware associated with Russian cyber-espionage campaigns.
- Sidenote: Heartbleed (CVE-2014-0160) earns an honorable mention as another celebrity vulnerability, even if it didn't quite make the grade with a Kenna severity score of 96.8.

2015

Adobe Flash & Juniper vulnerabilities

Adobe Flash took top honors with half of all 100 scored vulnerabilities in 2015. It's not much of a surprise that browsers and phones began blocking Flash by default and Adobe announced end-of-life for the product in 2017.

Another notable mention is the Juniper backdoor (CVE-2015-7755) in Netscreen firewalls that could lead to "complete compromise of the affected device."

2016

ZyXEL modem & DoS

- CVE-2016-10372 was a ZyXEL modem RCE vuln that put tens of thousands of Eir (Ireland's largest ISP) internet users at risk.
- CVE-2016-2776 the ISC (Internet Systems Consortium) discovered a Denial of Service (DoS) from a maliciously crafted DNS request.

2017

Petya ransomware & Apache Struts

- Petya ransomware started spreading globally, exploiting a MSFT SMB protocol vuln CVE-2017-0144 to infect host machines.
- The infamous Equifax Apache Struts vulnerability (CVE-2017-5638) made headlines and five other Apache Vulnerabilities were scored 100/100 in 2017 (CVE-2017-12617, CVE-2017-12635, CVE-2017-12636, CVE-2017-9791, CVE-2017-9805).

2018

Spectre, Meltdown, Drupal, Jenkins, Jquery and libissh vuln

- While Spectre (CVE-2017-5753, CVE-2017-5715) and Meltdown (CVE-2017-5754) made headlines in January of 2018, the massive industry response and relative difficulty of executing exploits didn't pop them up to the top of the risk scoreboard for the year.
- Instead the riskiest vulnerabilities involved RCE's in popular and widely used open source tools including Drupal (CVE-2018-7600, CVE-2018-7602), Jenkins (CVE-2018-1000861), Jquery (CVE-2018-9206), and an authentication bypass in libssh (CVE-2018-10933).

2019

BlueKeep

Who can forget Microsoft's latest and greatest RDP vulnerability BlueKeep (CVE-2019-0708)? BlueKeep was one of only six vulnerabilities that we rated 100/100 in 2019 and for good reason: the Kenna predictive algorithm noted that this would likely have an exploit (elevating the risk score to 96) and should be prioritized for remediation. The first attacks in the wild registered two months after the CVE was published. Read how we tracked this one here.

2020

MS Exchange and F5 Networks vulns

- 2020 follows in 2019's footsteps with a Microsoft Exchange RCE (CVE-2020-0688) that we have been tracking since it was revealed in February's Patch Tuesday. This one is unique as it is based on a static cryptographic key in a default application that is also exposed to the internet.
- F5 Networks' BIG-IP load balancing devices had an RCE (CVE-2020-5902) that was so risky that F5 noted that many devices were likely already compromised by the time they had published the vulnerability details and US CISA followed with their own advisory calling out ongoing attacks in the wild.

Defending your infrastructure? There's power in patterns.

The list of extremely critical vulnerabilities covers a mix of vendors, products and attack vectors. But the similarities between them highlight the strength of risk-based vulnerability management. Attackers follow well-worn pathways. While some CVEs may be more potent than others, the hackers who develop them can be somewhat predictable.

CVEs that allow remote code execution tend to draw a lot of interest. Likewise, vulnerabilities impacting certain operating systems and vendors are more likely to be weaponized. While these vulnerabilities represent the worst of the worst, they fit the overall pattern. Knowing that allows companies to stay ahead of the curve. By identifying vulnerabilities that are likely to be exploited, and then correlating that with their business context, security teams can effectively reduce overall risk for their organizations.

For even more information on modern vulnerability management solutions, or to see modern vulnerability management in action, visit **www.kennasecurity.com**

KENNA Security