CYBER THREAT ANALYSIS

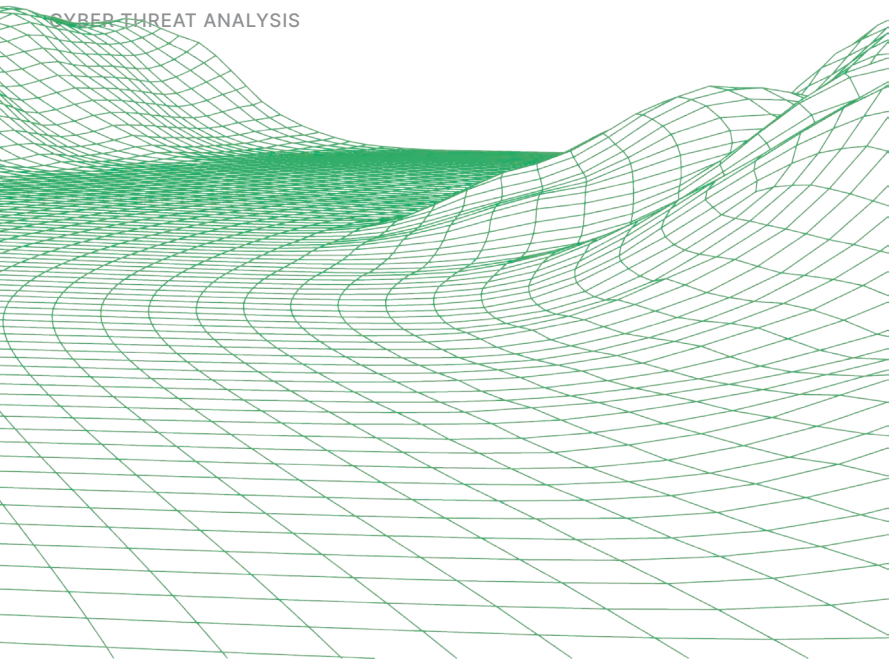
Recorded Future®

By Insikt Group®

CTA-2020-1103

Q3 2020 VULNERABILITY LANDSCAPE

Recorded Future®



This report examines high-risk vulnerabilities disclosed by major hardware and software vendors released from July 1 to September 30, 2020. Data was assembled from Recorded Future queries and public reporting on NVD data. This report does not attempt to summarize all vulnerabilities disclosed during this time period, but instead paints an overall picture of vulnerabilities disclosed in Q3 2020. Note that Recorded Future triggered risk rules are dynamic and apt to change after publication. Our client-only version of this report contains a full list of the vulnerabilities identified during the course of this research.

Executive Summary

Based on analysis of vulnerabilities disclosed between July 1 and September 30, 2020, Recorded Future identified 22 as the most high-risk vulnerabilities of the quarter, down approximately 50 percent from last quarter's 46. Recorded Future believes a variety of factors contributed to this marked decrease, including an overall lessened amount of vulnerabilities disclosed this quarter, although there was a slight increase in volume of recorded widespread malicious cyber threat activity compared to last quarter. These 22 vulnerabilities were determined based on a combination of CVSS v3.1 score, Recorded Future critical risk score, and number of references per vulnerability within the Recorded Future platform. This quarter, the top three vulnerabilities that pose the most risk for cyber exploitation are:

- CVE-2020-1472 (Zerologon) (impacts Microsoft)
- CVE-2020-1350 (SIGRed) (impacts Microsoft)
- CVE-2020-5902 (impacts F5 Big-IP Access Policy and Firewall Manager)

Key Judgments

- Last quarter, Recorded Future identified 46 of 3,846 disclosed vulnerabilities to be the most at-risk for cyber exploitation. This quarter, Recorded Future identified 22 of 3,233 disclosed vulnerabilities to be the most at-risk. The decrease in high-risk vulnerabilities from last quarter does not necessarily indicate a lessening of overall malicious activity, but does indicate a lesser volume of recorded cyber threat activity this quarter.
- Of the 22 top high-risk vulnerabilities, 10 impacted Microsoft, two impacted Apache, two impacted Cisco Jabber, one impacted F5 BIG-IP devices, one impacted McAfee, one impacted Citrix, and the remaining five impacted an even remaining spread of miscellaneous software. Consistent with the both previous quarters, Microsoft continued to be the top most heavily impacted product.
- Of the 22 top high-risk vulnerabilities, 17 have a confirmed publicly available POC, and eight are confirmed actively exploited in the wild.

Methodology

To assemble our data set of newly disclosed vulnerabilities for the quarter, we exported all vulnerabilities gathered from queries in the Recorded Future Platform that investigated newly disclosed vulnerabilities in July, August, and September 2020. Using the Recorded Future browser extension, we extracted all CVEs with a Recorded Future risk score of 75 or higher and identified a total of 22 vulnerabilities. The goal of this report is not to define every vulnerability disclosed over the past quarter, but to summarize the most significantly high-risk vulnerabilities, regardless of impacted products and software, to offer insights accessible from an overall landscape perspective.

Major Events and Trends

This quarter began with the disclosure of our third most high-risk vulnerability, CVE-2020-5902. First observed by Recorded Future and also disclosed by the National Institute of Standards and Technology (NIST) on July 1, 2020, **CVE-2020-5902** is a remote code execution vulnerability that impacts F5 BIG-IP devices. BIG-IP is a popular multi-purpose networking device with multiple functionalities, including balancers, firewalls, and access gateways, and is widely used in enterprise systems. Three days after disclosure, reports emerged of active exploitation, and US-CERT released an advisory confirming exploitation and reinforcing patch prioritization on July 24, 2020. As shown below, chatter around CVE-2020-5902 generally remained consistent throughout Q3 2020, with the vulnerability having the third highest number of references on this report's list (21,484).

Shortly after, **CVE-2020-1350 (SIGRed)** followed, having been first observed by Recorded Future and also disclosed by NIST on July 14, 2020. SIGRed is a remote code execution vulnerability in Microsoft DNS servers that impacts Windows servers from 2008 through the most recent version of Windows Server 2019. To exploit SIGRed, an attacker needs to send a specially crafted DNS response packet to a Windows Server running a vulnerable version of Microsoft's DNS. On July 16, 2020, security researcher Max Van Amerongen shared via social media his Github repository containing a denial of service (DoS) proof-of-concept (POC) exploit written in Python for the SIGRed vulnerability, and also included a short demo video of the exploit as well as a pcap of the exploit process. According to Recorded Future Malware Hunting, CVE-2020-1350 was observed being exploited as recently as July 25, 2020.

Finally, our number one vulnerability identified this quarter — with the highest CVSS v3.1 score possible, the highest Recorded Future risk score possible, and the highest number of references in Recorded Future (29,737) as compared to the other high-risk vulnerabilities identified this quarter — is **CVE-2020-1472 (Zerologon)**. Recorded Future data shows that Netlogon products are only impacted by one other critical vulnerability, CVE-2015-0005, indicating that Netlogon is not historically a strong target for attackers. Zerologon was reported by NIST on August 17, 2020, but it was not until early to mid-September 2020 that more media attention was given to the vulnerability, as shown in the timeline below. We believe that media attention surged nearly one month later mainly as a result of attackers developing exploits and attempting to exploit the vulnerability immediately following vulnerability disclosure. The reverse situation could also be true: as Zerologon began to receive media attention, more and more attackers likely jumped on the possibility of exploitation, perpetuating Zerologon's popularity among criminals. Both scenarios likely contribute to the fact that Zerologon is the number one most high-risk vulnerability for Q3 2020. Regarding the vulnerability itself, Zerologon is a privilege escalation vulnerability that takes advantage of a weak cryptographic algorithm used in the Netlogon authentication process. Attackers can exploit the vulnerability by establishing a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC).

Figure 1: Timeline view of Q3 2020's top three vulnerabilities. (Source: Recorded Future)

Figure 2: Timeline view of Q3 2020's top eight vulnerabilities. (Source: Recorded Future)

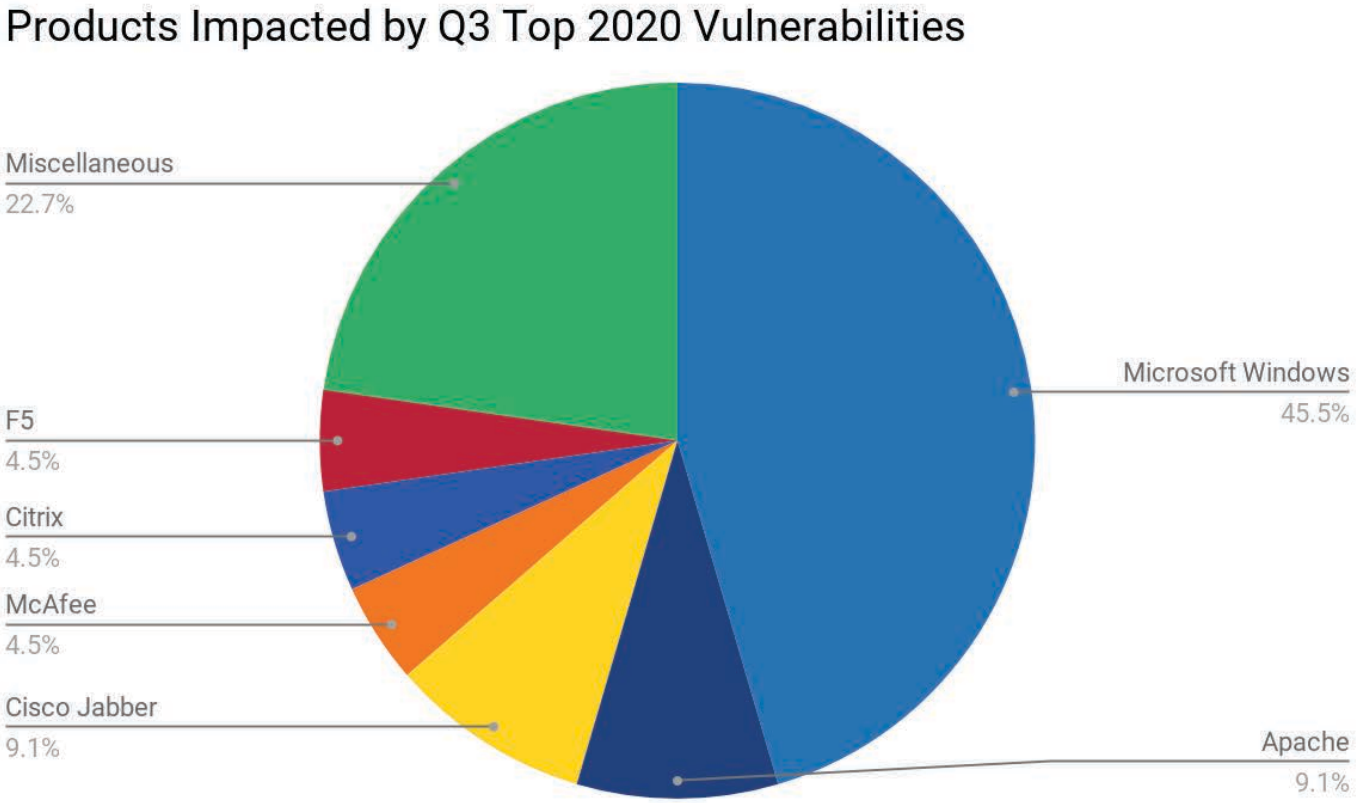


Figure 3: Chart of products impacted by Q2 2020's top 46 vulnerabilities.

Actively Exploited Vulnerabilities

Of the 22 vulnerabilities identified as high-risk for Q3 2020, eight have been reported by either open sources or Recorded Future Malware Hunting as actively exploited (approximately 36 percent). This does not mean that none of the other 14 have been exploited, just that eight are known based on public or private reporting. Of the eight actively exploited vulnerabilities, six impact Microsoft Windows, one impacts F5 BIG-IP devices, and one impacts VBulletin. Except for CVE-2020-1472 (Zerologon), CVE-2020-1350 (SIGRed), and CVE-2020-5902, which are detailed above, the actively exploited vulnerabilities are outlined below:

- **CVE-2020-17496:** A remote code execution vulnerability impacting popular forum software VBulletin. Exploitation of this vulnerability could grant an attacker privileged access and control over any vBulletin server running versions 5.0.0 up to 5.5.4, and even lock organizations out from their own websites. This vulnerability was first observed by Recorded Future on August 12, 2020, and reported as exploited by SonicWall Capture Labs on September 25, 2020.
- **CVE-2020-1147:** A remote code execution vulnerability impacting Windows .NET components (DataSet and DataTable), ultimately affecting Microsoft SharePoint and Visual Studio. To exploit this vulnerability, attackers would have to upload a specially crafted document to a server using an affected product to process content. This vulnerability was first observed by Recorded Future on July 14, 2020 and reported as exploited on October 6, 2020.
- **CVE-2020-1362:** An elevation of privilege vulnerability that impacts Windows WalletService and takes advantage of how the software handles objects in memory. To exploit this vulnerability, an attacker must run a specially crafted application. Successful exploitation could lead to attackers executing code with elevated permissions. This vulnerability was first observed by Recorded Future on July 14, 2020, and reported as exploited on September 17, 2020.
- **CVE-2020-1399:** An elevation of privilege vulnerability in Windows that occurs as a result of Windows Runtime being unable to handle objects in memory. An attacker who successfully exploits this vulnerability could run arbitrary code in an elevated context. Exploitation of this vulnerability would involve an attacker running a specially crafted application on the victim system. This vulnerability was first observed by Recorded Future on July 14, 2020 and reported as exploited on September 26, 2020.
- **CVE-2020-1374:** A remote code execution vulnerability that exists in Windows Remote Desktop Client when a user connects to a malicious server. Successful exploitation could allow an attacker to execute arbitrary code on the computer of the connecting client, as well as install programs, view, change, delete data, or create new accounts with full user rights. To exploit this vulnerability, an attacker must have control over a server and then convince a user to connect to it. Microsoft notes that an attacker must deceive the user into connecting, especially via social engineering, DNS poisoning, or using a Man-in-the-Middle (MITM) technique. This vulnerability was first observed by Recorded Future on July 14, 2020 and reported as exploited on July 29, 2020.

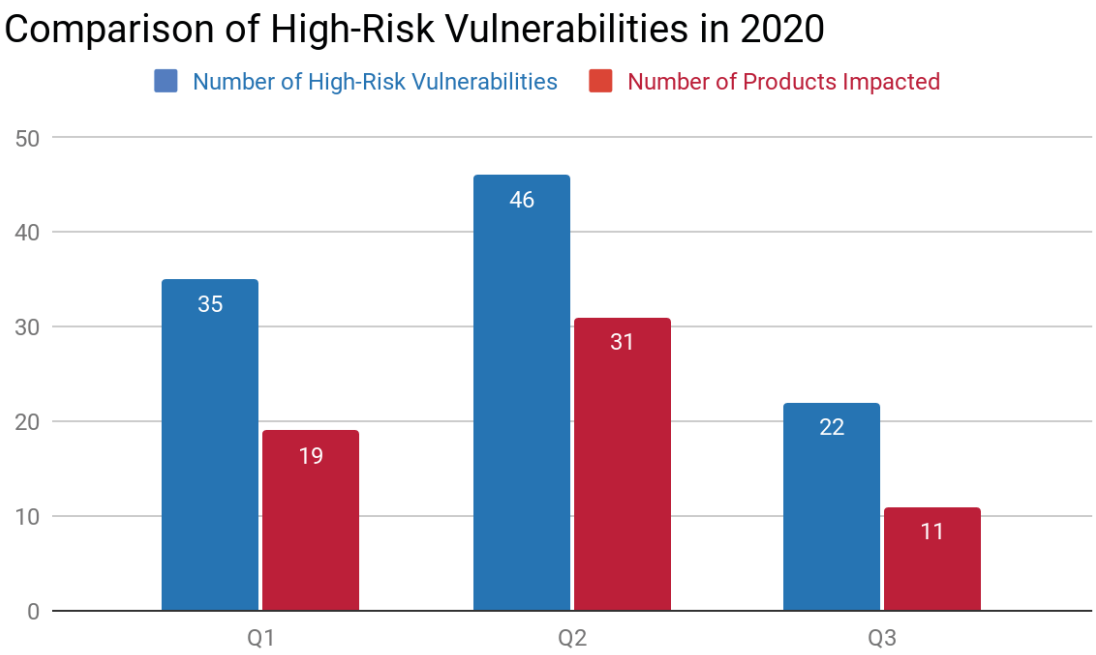


Figure 4: Chart examining a comparison of high-risk vulnerabilities and products impacted between quarters in 2020.

Proof-of-Concept Exploits

Of the 22 vulnerabilities identified as high risk for Q3 2020, 17 have been identified as having POC code. Overall, exploits with publicly released POCs pose less of a risk than already actively exploited vulnerabilities, but still maintain a medium-high level of risk, as threat actors can more easily take advantage of vulnerabilities with publicly disclosed POC code than vulnerabilities without. Of the 17 with released POC code, 11 had POC code published on GitHub, while the remaining six had POC code disclosed across open source security research websites or news media.

Outlook

Consistent with both prior quarters this year, Microsoft again maintained their number one spot as the most heavily targeted product for newly disclosed, critical vulnerabilities in Q3 2020, with Cisco and Apache tying for second, and a variety of other products tying for third, including McAfee, F5, and Citrix. Moving into Q4 2020, Recorded Future recommends administrators prioritize patching for Microsoft Windows servers, as the vulnerabilities in Microsoft products will likely continue to be the most targeted in Q4 2020.

What is most surprising about this quarter is the decrease in significant high-risk vulnerabilities compared to last quarter. Recorded Future believes this decrease may indicate attackers' preference to target well-known vulnerabilities, like our top three: CVE-2020-1472 (Zerologon),

CVE-2020-1350 (SIGRed), and CVE-2020-5902, each of which received a significantly high volume number of references across Recorded Future sources as compared to the number of references for the other 19 vulnerabilities.

Attackers are always looking for more effective and efficient means of targeting and exploiting enterprise networks. Any vulnerability that has publicly released POC code and has already been reported as actively exploited is much more attractive to an attacker than one without exploitation or publicly released POC code, as much of the work has already been done for them.

Looking at Q1, Q2, and Q3 2020, Recorded Future observed Q2 as having the most high-risk vulnerabilities, with Q1 following closely behind with 35 vulnerabilities and Q3 in third place with 22 vulnerabilities. The amount of products impacted are relatively proportional to the number of high-risk vulnerabilities disclosed each quarter. Although there is not enough evidence as of yet to estimate how many high-risk vulnerabilities will be identified in Q4, we can expect similar ratios for the number of high-risk vulnerabilities versus products impacted in Q4.

Security professionals often discuss the importance of defense in depth, but the trend in critical vulnerabilities across all three quarters this year demonstrates that there are flaws in all defense-in-depth points.

For example, in Q2 there were critical vulnerabilities against Cisco and Palo Alto. Cisco also had high-risk vulnerabilities in Q3, but so did F5 and RAD Secflow. These vulnerabilities could allow an attacker access to the periphery of an organization's network. There are also critical vulnerabilities in what are often internet-facing systems such as Apache in Q2 and Q3 and WordPress in Q1 and Q2.

Once inside the network, vulnerabilities in system management tools could make it easier for an attacker to move around the network. These tools include Eyes of Network in Q1, Citrix in Q2 and Q3 (Citrix is often used to gain initial access as well) and VMWare in Q1 and Q2.

Finally, with critical vulnerabilities in commonly deployed endpoint solutions — Trend Micro in Q1, Sophos in Q2 and McAfee in Q3 — attackers could potentially have access to any endpoint.

Overall, critical vulnerability trends this year demonstrate that all parts of an organization's technology stack are vulnerable and need to be monitored closely and patched quickly.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.