

Instant Recall of Flashpoint Intelligence with Polarity

Polarity is not a new dashboard to search or a new portal to manage. Instead, it works like Augmented Reality for security teams overlaying your existing workflows to enrich your view as you work. With Polarity you are better equipped to make thorough decisions and take action with speed.

Polarity helps you find the right data to make better decisions. It's about being thorough; knowing what is available from past analysis completed by you and your teammates, as well as all the context provided by the security products used day-to-day. The Polarity open-source integration framework supports more than 150 security products including Flashpoint.

Polarity's integration with Flashpoint enables the analyst with instant recall of information from the Flashpoint Intelligence Platform related to CVE ID's, Email Addresses, IP Addresses, Web Domains, and File Hashes.

When integrated with Polarity, Flashpoint intelligence and indicator metadata is overlaid on the analyst's screen while they work within any client-side application. For example, indicator metadata, intelligence reports, and underground forum post transcripts are automatically overlaid on screen via the Polarity overlay window while viewing an email that contains a CVE ID as shown below.

Search entities in Polarity

On-demand only Stream Highlight

CVE-2020-0796 Q

FP Indicator Count: 1 FP CVSSv2 Base Score: 7.5
FP CVSSv3 Base Score: 10

Flashpoint

Indicators Reports (10) Posts (10)

Indicator Detail

Indicator Name: [CVE-2020-0796](#)

MITRE Description: A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

MITRE Created At: 2019-11-03 19:00:00 EST
MITRE Last Observed At: 2020-12-11 14:00:02 EST
NIST NVD Created At: 2020-03-12 12:15:00 EDT
NIST NVD Last Observed At: 2020-06-19 16:00:02 EDT

CVSS v2 Detail:

Complexity: LOW
Complexity: LOW
Vector: NETWORK
Authentication: NONE
Availability Impact: PARTIAL
Base Score: 7.5
Confidentiality Impact: PARTIAL
Exploitability Score: 10
Impact Score: 6.4
Integrity Impact: PARTIAL
Severity: HIGH
Vector String: [AV:N/AC:L/Au:N/C:P/P:A/P](#)

CVSS v3 Detail:

Availability Impact: HIGH
Base Score: 10
Confidentiality Impact: HIGH
Exploitability Score: 3.9
Impact Score: 6
Integrity Impact: HIGH
Privileges Required: NONE
Scope: CHANGED

Search entities in Polarity

On-demand only Stream Highlight

CVE-2020-0796 Q

Flashpoint

Report Detail

Title: [CVE-2020-1206 \(SMBv3\)](#)

Summary: While investigating [CVE-2020-0796](#) (GhostSMB), security researchers at ZecOps discovered a new vulnerability in the same function of SMBv3, which could result in remote information disclosure.

Posted: 2020-06-25T14:37:03.328+00:00
Last Updated: 2020-06-25T14:37:03.328+00:00

Report Tags

Technology & Internet Intelligence Report Global
Exploits & Vulnerabilities Cybersecurity & Internet Governance

Report Detail

Title: [Daily Standup - 06.09.2020](#)

Posted: 2020-06-09T16:03:48.564+00:00
Last Updated: 2020-06-09T16:03:48.564+00:00

Report Tags

Standup

Report Detail

Title: [Trending Vulnerabilities: May 2020](#)

Summary: In May 2020 analysts observed threat actors in Flashpoint's forum datasets discuss a total of 292 unique vulnerabilities.

Posted: 2020-06-03T22:49:19.216+00:00
Last Updated: 2020-06-03T22:49:19.216+00:00

Report Tags

Exploits & Vulnerabilities Cybersecurity & Internet Governance
Technology & Internet Global Intelligence Report
Cyber Threats

Search entities in Polarity

On-demand only Stream Highlight

CVE-2020-0796 Q

Flashpoint

Forum Posts Detail

Pivot to Thread

Published At: 2020-12-10T23:22:00+00:00

Приветствую всех, кто читает эту статью. Это время я бы хотел удалить одной очень интересной уязвимости на мой взгляд.

Удаленное выполнение кода POC
Именно такое описание получила уязвимость [CVE-2020-0796](#).
Давайте взглянем на краткую сводку нашей проблемы. А именно:

- Дата появления: 10 марта 2020 года.
- Уязвимые системы: Windows 10 с версии 1903 до 1909.
- Тип: RCE (удаленное выполнение вредоносного кода).

Теперь идем к тому, как это все работает. У данной уязвимости имеется свой эксплоит, но для начала взглянем на схему работы, что я делал специально для статьи:

Попытался все сделать моментально понятно. Из "схемы" выше можно сделать вывод о том, что у нас происходит создание защищенного соединения от пользователя при помощи Netcat на порту 4321. Так же разберем флаги, что используются для создания:

- i режим прослушивания.
- v вывод информации о процессе работы.
- r (номер) локальное число для прослушивания.

Сам же уязвимость связана с тем, что протокол Microsoft Server Message Block версии 3.1.1 обрабатывает определенные запросы с помощью которых злоумышленник может получить удаленное управление системой. От теории к практике, попытаемся эксплуатировать нашу уязвимость.

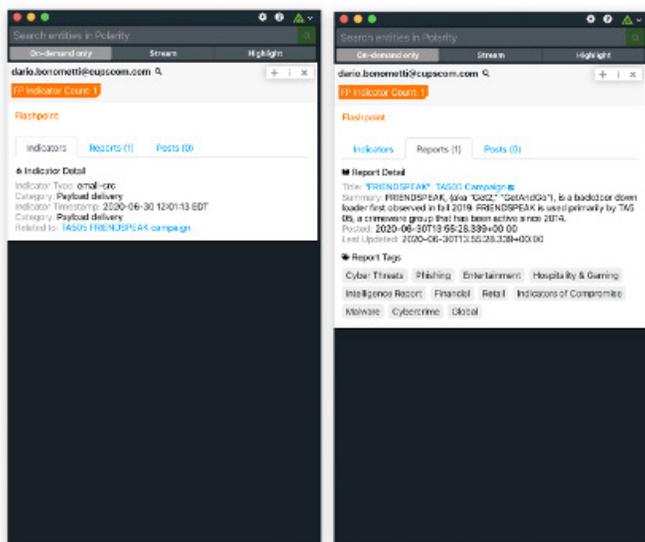
Эксплуатация CVE
Сам эксплоит, что нам понадобится размещен как всегда на GitHub. Скачиваем его и разархивируем. Для машины жертвы нужно запустить bat-файл:

После устанавливаем сам Netcat, короткая инструкция ниже.

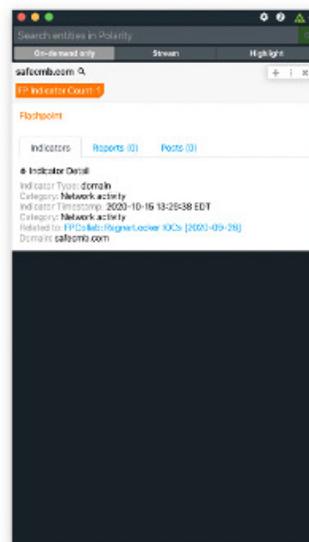
Windows:
1. Скачиваем программу [Download]

There are several pivot points illustrated below that enable analysts to rapidly link out to the Flashpoint fp.tools platform from the Polarity overlay window to perform additional research.

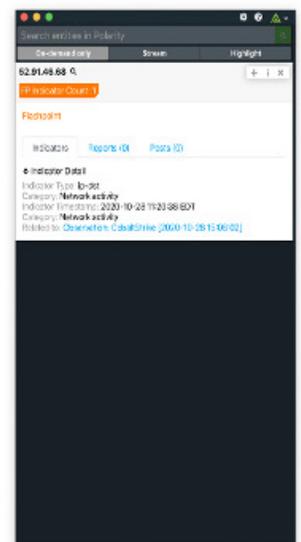
Email Address Enrichment



Web Domain Enrichment



IP Address Enrichment



Polarity helps analysts get the data needed to act quickly. It's about working fast; having the ability to retrieve relevant context exactly when it is needed to make a decision. Teams reporting being able to work 3 – 5 times faster when using Polarity with their security tools.

FLASHPOINT

Flashpoint delivers converged intelligence and risk solutions to private and public sector organizations worldwide.

As the global leader in Business Risk Intelligence (BRI), Flashpoint provides meaningful intelligence to assist organizations in combating threats and adversaries.

Through sophisticated technology, advanced data collections, and human-powered analysis, Flashpoint is the only intelligence firm that can help multiple teams across an organization bolster cybersecurity, confront fraud, detect insider threats, enhance corporate and physical security, improve executive protection, address third-party risk, and support due diligence efforts.

POLARITY

Data tells a story, Polarity helps you see it with software-based Augmented Reality overlaying contextual information as you work. No glasses or goggles are needed. When analysts use Polarity, they are better equipped to make thorough decisions and take action with speed.