Qualys Security Advisory: SolarWinds / FireEye

By Mehul Revankar

Published: 2020-12-22 · Archived: 2026-04-05 22:06:02 UTC

Qualys Researchers found Millions of devices exposed to vulnerabilities used in the stolen FireEye Red Team tools and SolarWinds Orion by analyzing the anonymized set of vulnerabilities across Qualys' worldwide customer base

Qualys to offer a free 60-day integrated Vulnerability Management, Detection and Response service to help organizations quickly assess the devices impacted by SolarWinds Orion vulnerabilities, SUNBURST Trojan detections, or FireEye Red Team tools, and to remediate them and track their remediation via dynamic dashboards. Register at https://www.qualys.com/solarhack/

On Dec 8, FireEye disclosed the theft of its Red Team assessment tools which leverage over 16 known CVE's to exploit client environments to test and validate their security posture. FireEye also confirmed a trojanized version of SolarWinds Orion software was used to facilitate this theft.

Access to these sophisticated FireEye Red Team tools stolen by the attackers increases the risk of an attack on an organization's critical infrastructure. Red teams often use a known set of vulnerabilities to exploit and quickly compromise systems to simulate what a real attacker can do in the network. If these tools fall into the wrong hands, it will increase the chances of successfully exploiting the vulnerabilities.

Why is this security incident so important?

To underscore the seriousness of this breach, the Department of Homeland Security has issued an emergency directive ordering all federal agencies to take immediate steps in mitigating the risk of SolarWinds Orion applications and other security vulnerabilities related to the stolen FireEye Red Team tools. They've also strongly recommended that commercial organizations adhere to the same guidance.

7+ million vulnerable instances open to potential attack across networks of global organizations analyzed by Qualys researchers

The Qualys Cloud Platform is the most widely used platform for Vulnerability Management by global organizations. Qualys Vulnerability Research Teams continuously investigate vulnerabilities being exploited by attackers. Since the public release of this information by FireEye and SolarWinds, our researchers have analyzed the state of these anonymized vulnerabilities across networks of organizations using Qualys Cloud Platform. While the number of vulnerable instances of SolarWinds Orion are in the hundreds, our analysis has identified over 7.54 million vulnerable instances related to FireEye Red Team tools across 5.29 million unique assets, highlighting the scope of the potential attack surface if these tools are misused. Organizations need to move quickly to immediately protect themselves from being exploited by these vulnerabilities.

The good news is that patches have been available for these vulnerabilities for some time. Interestingly, further analysis of those 7.54 million vulnerable instances indicated about 7.53 million or roughly 99.84% are from only

eight vulnerabilities in Microsoft's software as listed below. Luckily Microsoft patches have been available for a while.

List of 8 patchable security vulnerabilities to significantly reduce attack surface

CVE ID	Release Date	Name	CVSS	Qualys QID(s)
CVE-2020-1472	08/11/2020	Microsoft Windows Netlogon Elevation of Privilege Vulnerability	10	91668
CVE-2019-0604	02/12/2019	Microsoft Office and Microsoft Office Services and Web Apps Security Update February 2019 Microsoft SharePoint	9.8	110330
CVE-2019-0708	05/14/2019	Microsoft Windows Remote Desktop Services Remote Code Execution Vulnerability (Blue. Keep)	9.8	91541, 91534
CVE-2014-1812	05/13/2014	Microsoft Windows Group Policy Preferences Password Elevation of Privilege Vulnerability (KB2962486)	9	91148, 90951
CVE-2020-0688	02/11/2020	Microsoft Exchange Server Security Update for February 2020	8.8	50098
CVE-2016-0167	04/12/2016	Microsoft Windows Graphics Component Security Update (MS16-039)	7.8	91204
CVE-2017-11774	10/10/2017	Microsoft Office and Microsoft Office Services and Web Apps Security Update October 2017	7.8	110306
CVE-2018-8581	11/13/2018	Microsoft Exchange Server Elevation of Privilege Vulnerability	7.4	53018

* See the full list of 16 exploitable vulnerabilities and their patch links.

Recommended action to mitigate the risk immediately

Based on sheer risk and scale of these vulnerabilities, it is imperative for organizations to quickly assess the state of these vulnerabilities and missing patches across all their assets impacted by SolarWinds Orion vulnerabilities, SUNBURST Trojan detections, or FireEye Red Team tools.

- Immediately deploy applicable patches for all above vulnerabilities across the affected assets.
- Power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from the network, until patch – is applied.
- Apply security hygiene controls for the impacted software and operating system to reduce the impact.

- Search for existence of the following files:
    - [SolarWinds.Orion.Core.BusinessLayer.dll] with a file hash of [b91ce2fa41029f6955bff20079468448]
    - [C:\WINDOWS\SysWOW64\netsetupsvc.dll]

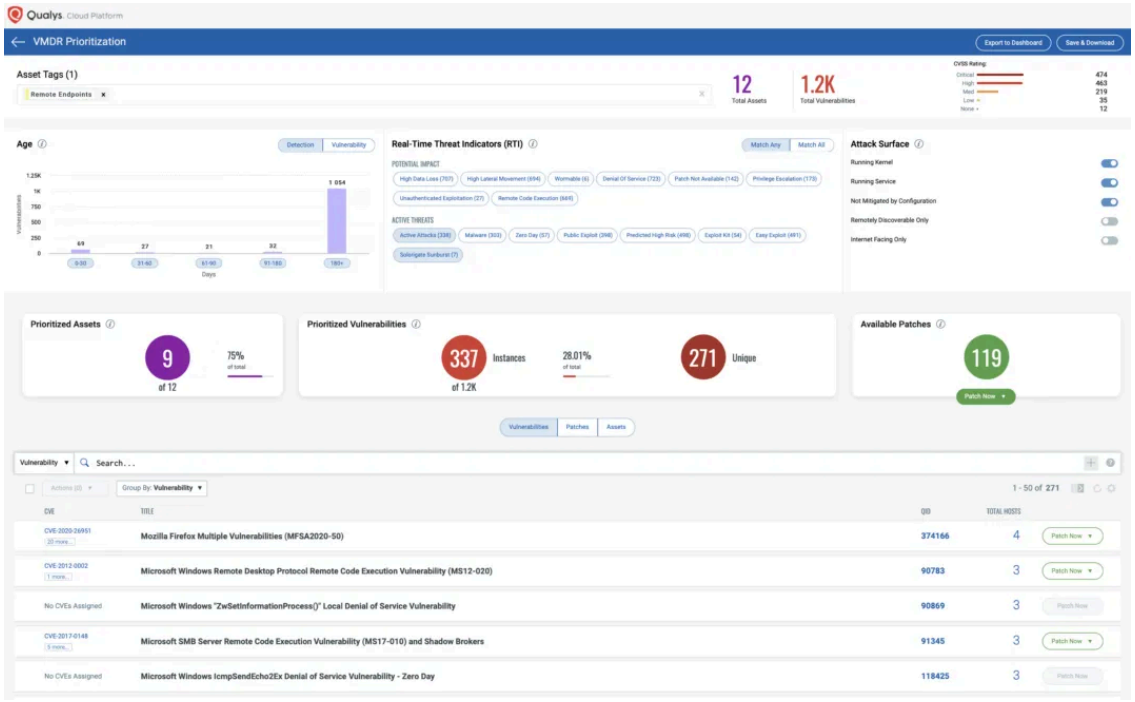
and other Indications of Compromise, and remove them along with killing the parent processes that touched them.

Qualys brings free 60-day integrated Vulnerability Management, Detection and Response service to detect and patch these vulnerabilities

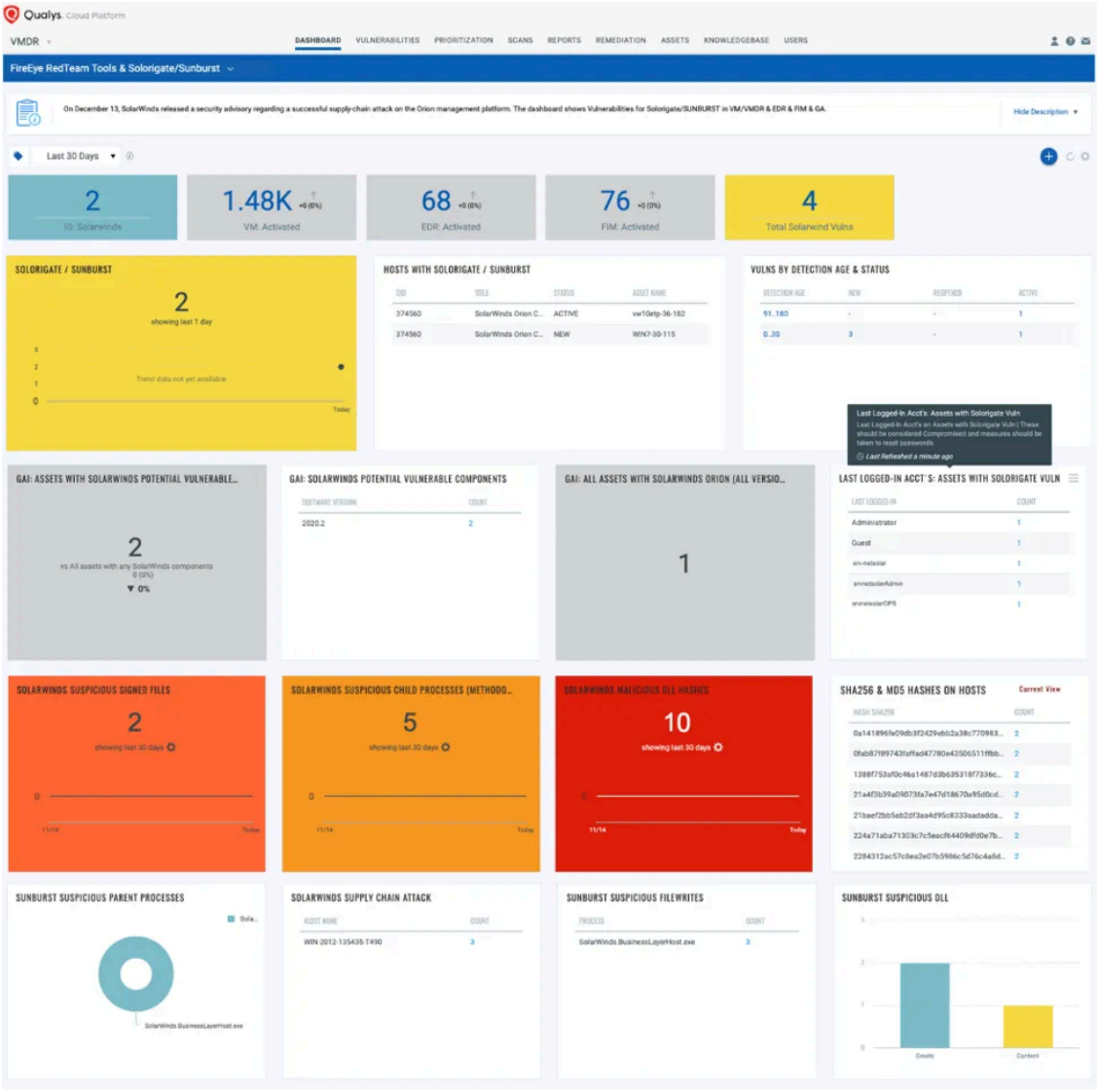
To help global organizations, Qualys is offering a free service for 60 days, to rapidly address this risk. The service enables customers with –

- Real-time, up-to-date inventory and automated organization of all assets, applications, services running across the hybrid-IT environment
- Continuous view of all critical vulnerabilities and their prioritization based on real-time threat indicators and attack surface
- Automatic correlation of applicable patches for identified vulnerabilities
- Patch Deployment via Qualys Cloud Agents with zero impact to VPN bandwidth
- Security configuration hygiene assessment to apply as compensating controls to reduce vulnerability risk
- Unified dashboards that consolidate all insights for management visualization via a single pane of glass

In addition to Qualys VMDR and Patch Management, organizations can also leverage additional capabilities like EDR and FIM to detect additional indicators of compromise such as malicious files, hashes and remove them from their environment.



VMDR prioritization screen with Solorigate SUNBURST RTI selected



Qualys Unified Dashboard showing FireEye Red Team tools & Solorigate/SUNBURST risk

Existing Qualys customers can immediately leverage their accounts to mitigate their exposure for recommended actions

- Inventory the compromised versions of SolarWinds and VMware applications as well as other actively running services, and processes.
- Detect all applicable vulnerabilities related to Solorigate/SUNBURST, FireEye tools as well as VMware applications along with a prioritized list of appropriate patches to deploy.
- Immediately deploy prioritized patches for the above critical vulnerabilities. In case a patch cannot be applied immediately, it leverages the compensating controls to reduce the risk impact until patches can be applied.
- Additionally, it can detect for the evidence of malicious files and IOCs related to SolarWinds applications and FireEye compromised toolsets and remove them.

Additional resources

- CISA Emergency Directive 21-01

- SolarWinds Security Advisory
- FireEye Red Team tools countermeasures
- Qualys Research on FireEye Theft
- Qualys Research on SolarWinds
- How to quickly deploy Qualys cloud agents for Inventory, Vulnerability and Patch Management

---