MALWARE

SOLARWINDS ORION

About: A vulnerability in API that allowed attackers to bypass authentication that lead to Remote Command Execution. Recent instance of this malware was in 2020.

Attack type
Ability to run commands through an API

Target
Solarwinds Orion server

Impact
Loss of sensitive data, impact on availability, loss of productivity

The attack skips authorizations when using API with hidden parameter

STEP 1
API request to these endpoints: WebResource.axd, ScriptResource.axd, i18n.ashx, or Skipi18n with PathInfo parameter disables authorizations

STEP 2
Attackers can perform remote code execution and upload SUPERNOVA malware

STEP 3
Attackers can trigger actions on the malware and extract sensitive data silently

TARGETED ATTACK

FULL PROTECTION OF WEB APPLICATIONS AND APIS

ROHDE & SCHWARZ CYBERSECURITY WAF TECHNOLOGIES

The solution that provides proven protection for applications and servers against remote web attack

Application Whitelist (sitemap) protects API. The malware is neutralized

Application whitelist detects the use of PathInfo hidden parameter and blocks it (or other unknown parameters – SUNBURST). Alternatively, adding a specific rule to security engines would block the use of this parameter

No actions or upload performed on remote application. Data and applications are safe

IMMEDIATE TOTAL PROTECTION

R&S®Web Application Firewall
The comprehensive solution is offering a multilayered approach to web application security by dynamically detecting and blocking malicious content while efficiently transmitting legitimate traffic at enterprise level

R&S®Cloud Protector
A true SaaS solution to address the security issues of the application layer in the cloud. It effectively protects your web applications from the most common cyberattacks without consuming critical internal resources. With easy configuration and management, it provides greater security at a lower lifetime cost (TCO)

R&S®Trusted Application factory
A cloud native application protection solution, running in a container, which scales with the app, decreases false positive rate and data loss risk while increasing DevSecOps agility and performance

▸ **For more related content, please join our community website: https://dev-appsec.rohde-schwarz.com**

ROHDE&SCHWARZ
Make ideas real