



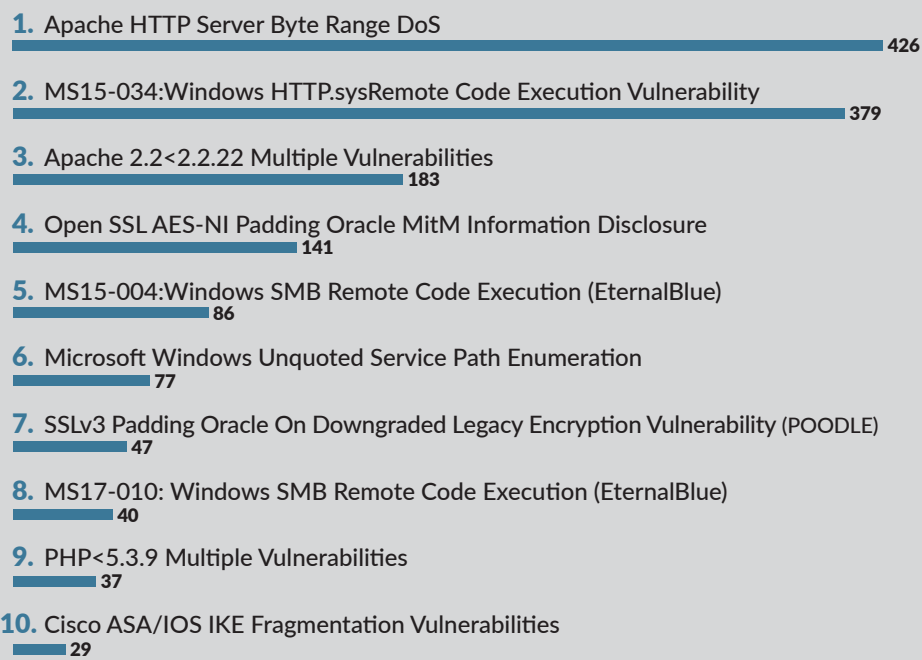
# 2018 Security Threat Report

## Assessing Nine Years of Cyber Security Vulnerabilities and Exploits

Disclosures of significant cyber security breaches have become routine as organizations increasingly rely on vulnerable digital technologies and third-party service providers. Protiviti's *2018 Security Threat Report* aims to help organizations address and understand the cyber security landscape by exploring and detailing the most common digital threats today.

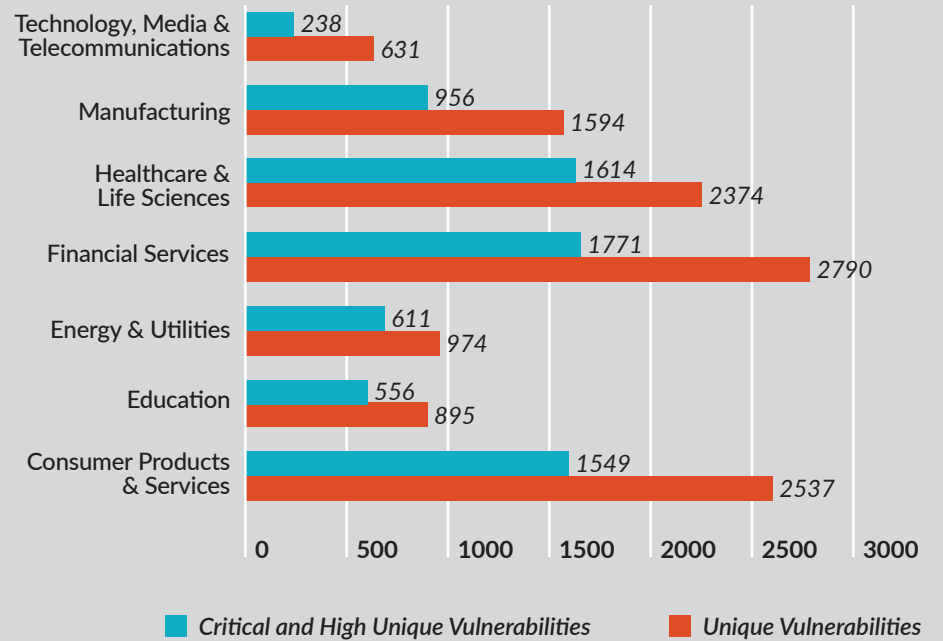
**Missing Microsoft patch MS17-010, which WannaCry used as a transport method, cracked the list of top 10 external exploits in less than a year.**

### Top 10 External Exploits



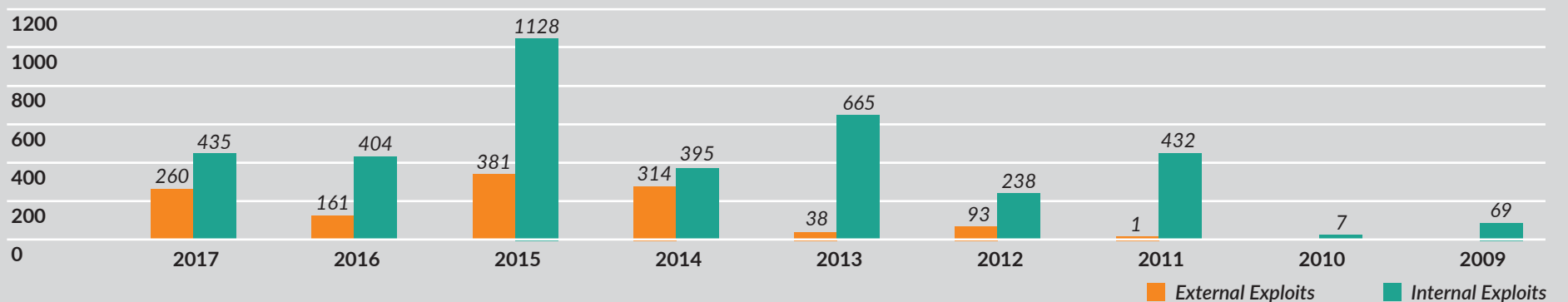
**Technology, Media and Telecommunications organizations had the lowest percentage of vulnerabilities that were "critical" or "high" in severity.**

### Vulnerability Severity by Industry

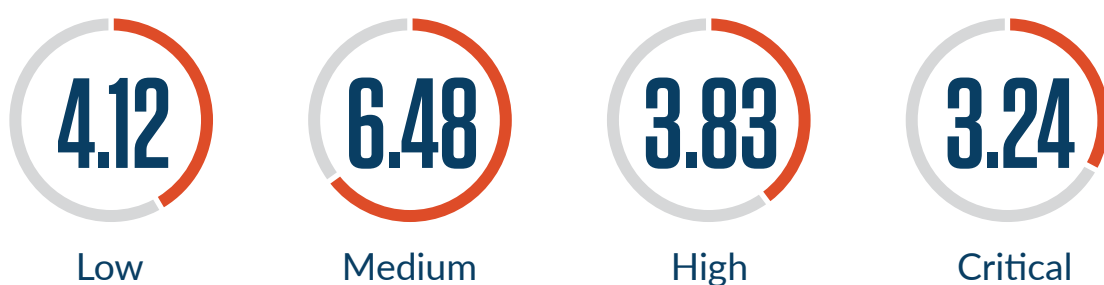


**Internal networks contain many more exploitable vulnerabilities compared to external networks.**

### Number of External vs. Internal Infrastructure Exploits by Year



### Average Age of Vulnerabilities (Years) by Severity, from 2017 to Vulnerability Release Date



### Key calls to action:

- Strong permission and user access controls
- Employee security awareness
- Patch management
- System configuration management
- Periodic penetration testing

Protiviti compiled the data, analyses and trends presented in this report by reviewing information from security vulnerability scans of IT systems of more than 500 organizations in a broad range of industries. Learn more by reading Protiviti's *2018 Security Threat Report*, available at [Protiviti.com/ThreatReport](http://Protiviti.com/ThreatReport).