

Vulnerability Research & Advisor

Finalità e modalità operative

Nell'ambito delle attività di Cybersecurity di TIM, è stato costituito un gruppo di lavoro dedicato all'esecuzione di Security Assessment (Red Team), che si occupa di analizzare software sviluppato on-demand, software di mercato e firmware.

Tra gli obiettivi del team c'è quello di rilevare le vulnerabilità che un potenziale attaccante potrebbe sfruttare per eseguire degli attacchi informatici verso le infrastrutture di TIM ed evidenziarne gli impatti reali rilevati.

L'attività non si limita alla sola verifica delle vulnerabilità note, ma include un'attività di ricerca specifica con l'obiettivo di scoprire eventuali nuove vulnerabilità non ancora conosciute pubblicamente (vulnerabilità Oday).

Qualora vengano rilevate vulnerabilità Oday, si procede con una “divulgazione responsabile” verso il produttore del prodotto analizzato, comunicandogli prontamente e in via confidenziale le vulnerabilità scoperte, in modo che possa replicarle e produrre una contromisura (patch) entro 90 giorni dalla notifica ricevuta.

In seguito al rilascio della contromisura (patch), oppure trascorsi i 90 giorni dalla segnalazione, si procede alla pubblicazione, classificando le vulnerabilità sul Mitre (CVE, Common Vulnerabilities and Exposures).

Analoghe azioni vengono intraprese nell'ambito dei processi di Security Testing e Gestione Incidenti (Incident Handling) di TIM, qualora portino a scoprire vulnerabilità non ancora note al produttore e alla comunità.

CVE-2022-40715 – Nokia 1350 OMS Optical Management System

CVE-2022-40714 – Nokia 1350 OMS Optical Management System



CVE-2022-40712 – Nokia 1350 OMS Optical Management System	+
CVE-2022-39821 – Nokia 1350 OMS Optical Management System	+
CVE-2022-39819 – Nokia 1350 OMS Optical Management System	+
CVE-2022-39817 – Nokia 1350 OMS Optical Management System	+
CVE-2022-39816 – Nokia 1350 OMS Optical Management System	+
CVE-2022-39815 – Nokia 1350 OMS Optical Management System	+
CVE-2022-39814 – Nokia 1350 OMS Optical Management System	+
CVE-2022-39810 – WSO2 Enterprise Integrator	+
CVE-2022-39809 – WSO2 Enterprise Integrator	+
CVE-2022-29540 – RESI S.p.A	+
CVE-2022-29539 – RESI S.p.A	+
CVE-2022-29538 – RESI S.p.A	+
CVE-2022-28866 – Nokia AirFrame BMC	+
CVE-2022-28862 – ARCHIBUS Web Central	+



CVE-2022-27880 – F5 Traffix Signal Delivery Controller



CVE-2022-27662 – F5 Traffix Signal Delivery Controller



CVE-2022-26484 – Veritas Operations Manager



CVE-2022-26483 – Veritas Operations Manager



CVE-2022-25344 – Olivetti d-COLOR MF3555



CVE-2022-25343 – Olivetti d-COLOR MF3555



CVE-2022-25342 – Olivetti d-COLOR MF3555



CVE-2021-43080 – Fortinet FortiOS



CVE-2021-41555 – ARCHIBUS Web Central



CVE-2021-41554 – ARCHIBUS Web Central



CVE-2021-41553 – ARCHIBUS Web Central



CVE-2021-38123 – Micro Focus Network Automation



CVE-2021-36200 – Johnson Controls Metasys MREWeb Service



CVE-2021-35492 – Wowza Streaming Engine





----- WOWZA Streaming Engine

CVE-2021-35490 – Thruk



CVE-2021-35489 – Thruk



CVE-2021-35488 – Thruk



CVE-2021-35487 – Nokia Broadcast Message Center



CVE-2021-32571 – Ericsson OSS-RC



CVE-2021-32570 – Ericsson Network Manager



CVE-2021-32569 – Ericsson OSS-RC



CVE-2021-31540 - WOWZA Streaming Engine



CVE-2021-31539 - WOWZA Streaming Engine



CVE-2021-29661 – Softing AG OPC Toolbox



CVE-2021-29660 – Softing AG OPC Toolbox



CVE-2021-28979 - Thales SafeNet KeySecure Management Console



CVE-2021-28488 – Ericsson Network Manager





CVE-2021-28249 – CA eHealth Performance Manager



CVE-2021-28248 – CA eHealth Performance Manager



CVE-2021-28247 – CA eHealth Performance Manager



CVE-2021-28246 – CA eHealth Performance Manager



CVE-2021-26597 – NOKIA NetAct



CVE-2021-26596 – NOKIA NetAct



CVE-2021-3314 - Oracle GlassFish Server

CVE-2021-2005 – ORACLE Business Intelligence Enterprise Edition of Oracle Fusion
Middleware

CVE-2020-35590 – WordPress Plugin Limit Login Attempts Reloaded



CVE-2020-35589 – WordPress Plugin Limit Login Attempts Reloaded

CVE-2020-28209 – Schneider Electric StruxureWare Building Operation Enterprise Server
Installer – Enterprise Central Installer

CVE-2020-27583 – IBM InfoSphere Information Server



CVE-2020-17458 – MultiUX





----- CVE-2020-15794 - Siemens Desigo Insight

CVE-2020-15794 – Siemens Desigo Insight



CVE-2020-15793 – Siemens Desigo Insight



CVE-2020-15792 – Siemens Desigo Insight



CVE-2020-14843 – ORACLE Business Intelligence Enterprise Edition of Oracle Fusion Middleware



CVE-2020-14842 – ORACLE Business Intelligence Enterprise Edition of Oracle Fusion Middleware



CVE-2020-14690 – ORACLE Business Intelligence Enterprise Edition of Oracle Fusion Middleware



CVE-2020-12081 – FlexNet Publisher



CVE-2020-9050 – Johnson Controls Metasys MREWeb Service



CVE-2020-7573 – Schneider Electric StruxureWare Building Operation WebReports



CVE-2020-7572 – Schneider Electric StruxureWare Building Operation WebReports



CVE-2020-7571 – Schneider Electric StruxureWare Building Operation WebReports



CVE-2020-7570 – Schneider Electric StruxureWare Building Operation WebReports



CVE-2020-7569 – Schneider Electric StruxureWare Building Operation WebReports





CVE-2020-2505 – QNAP QES



CVE-2020-2504 – QNAP QES



CVE-2020-2503 – QNAP QES



CVE-2019-19994 - Selesta Visual Access Manager



CVE-2019-19993 - Selesta Visual Access Manager



CVE-2019-19992 - Selesta Visual Access Manager



CVE-2019-19991 - Selesta Visual Access Manager



CVE-2019-19990 - Selesta Visual Access Manager



CVE-2019-19989 - Selesta Visual Access Manager



CVE-2019-19988 – Selesta Visual Access Manager



CVE-2019-19987 - Selesta Visual Access Manager



CVE-2019-19986 - Selesta Visual Access Manager



CVE-2019-19456 - WOWZA Streaming Engine



CVE-2019-19455 - WOWZA Streaming Engine



CVE-2019-19454 - WOWZA Streaming Engine



CVE-2019-19453 - WOWZA Streaming Engine



CVE-2019-17406 - NOKIA IMPACT



CVE-2019-17405 - NOKIA IMPACT



CVE-2019-17404 - NOKIA IMPACT



CVE-2019-17403 - NOKIA IMPACT



Gruppo
Investitori
Sostenibilità
Newsroom
Centro Studi
Lavora con noi
Contatti

I siti del Gruppo
Vendors Hub



[Privacy](#) [Note Legali](#) [Tutela minori & Segnalazioni](#) [Dichiarazione di accessibilità](#) [Responsible Disclosure](#)
[Vulnerability Research](#)

©2020 Telecom Italia - Partita IVA: 00488410010