OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 19.10.2026, 16:17 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	19.10.2026
Herausgeber	Maximilian Gilg, OT-Cyber.de, Rosenheim
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen
Online	https://ot-cyber.de/ot-lage/

Dieses Lagebild fasst öffentlich zugängliche Meldungen zusammen – automatisch zusammengestellt, ohne Gewähr. Die Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen in Deutschland, Österreich und der Schweiz.

Management Summary

Diese Ausgabe enthält 5 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

• **Loxone (Kollerschlag, Österreich): Cyberangriff am Wochenende auf den Hersteller von Gebäudeautomation**: Laut Florian Wöss aus der Geschäftsführung kamen die Angreifer über einen Webserver von Loxone herein (ORF Oberösterreich, 19.10.). Nach Angaben von Loxone sind das interne CRM, das Bewerbermanagement und die Datenbank der Webseite betroffen. Die Systeme wurden isoliert und werden schrittweise wieder hochgefahren. Kopiert wurden laut Loxone Kontaktdaten von Partnerbetrieben (vor allem Elektroinstallateure), Support-Anfragen und Bewerberdaten, ein Teil davon veraltet. Gegenüber dem ORF sprach Wöss zusätzlich von abgeflossenen Kundendaten, ohne Art oder Umfang zu nennen; die schriftliche Stellungnahme bei heise nennt nur Partner-, Support- und Bewerberdaten. Zugangsdaten von Kundenanlagen liegen laut Hersteller nur lokal auf dem Miniserver. Miniserver, Remote Connect und Exosphere seien nicht betroffen, Zahlungsdaten und Quellcode ebenfalls nicht. Loxone hat die Behörden informiert und arbeitet mit externen Forensikern. Auf der verunstalteten Webseite bekannte sich die Gruppe „Samurai“ und behauptet, rund 200 GB kopiert zu haben (heise). Laut Auflistung der Angreifer (Screenshots im Loxforum) sollen auch Daten zu Microsoft-365-Konten und SSO-Logins dabei sein, dazu ein Register mit rund 300.000 Miniserver-Seriennummern und Projektnamen. Loxone hat diese Angaben nicht bestätigt. Zur Confluence-Auflistung erklärt Loxone, das LoxWiki sei ein Community-Projekt, Loxone setze kein Confluence ein. Zu einer Lösegeldforderung sagt Loxone nichts. Unsere Einschätzung: Die abgeflossenen Partnerdaten könnten gezieltes Phishing über Elektroinstallateure an Betreiber von Gebäuden und technischen Anlagen ermöglichen. Betreiber sollten prüfen, ob ihre Miniserver aus dem Internet erreichbar sind, vorsorglich wegen der behaupteten SSO- und Seriennummern-Daten die Passwörter wechseln und ihre Installateure vor gefälschten Loxone-Mails warnen. Quellen: https://www.heise.de/news/Loxone-Cyberangriff-auf-Gebaeudeautomatisierungsanbieter-11492872.html · https://ooe.orf.at/stories/3375871/

• □ UPDATE: **Fortinet FortiManager und FortiOS: Unit 42 beschreibt Einbruch bei einem MSP und die Backdoor PEERSTITCH (CVE-2024-47575, CVE-2025-61624)**: Laut Unit 42 von Palo Alto Networks (Bericht vom 14.10.) ist die Gruppe CL-STA-0954 (auch UNC5820) ab September 2024 über FortiJump (CVE-2024-47575) in den FortiManager eines Managed Service Providers aus der Telekommunikation eingedrungen, der über 500 FortiGates verwaltet. Abgezogen wurden die Running-Configs dieser FortiGates, Topologie- und Routing-Daten, administrative, lokale und SSL-VPN-Zugangsdaten (als umkehrbar verschlüsselter Text gespeichert, einige Passwörter wurden laut Unit 42 per Brute Force geknackt) sowie Zertifikate mit privaten Schlüsseln. Die Netze der Endkunden hat Unit 42 nicht untersucht, dort ist nur der Abfluss von Konfigurationen und Zugangsdaten belegt, kein Einbruch. Über die Path-Traversal-Lücke CVE-2025-61624 (setzt eine Anmeldung voraus) schreiben die Angreifer als root Dateien und setzen die Backdoor PEERSTITCH ein. Sie hinterlässt kein dauerhaftes Binary auf der Festplatte (die Staging-Dateien lagen vorher unter /data2/template/), hängt sich per ptrace in die FortiOS-Prozesse iked und miglogd und lässt markierte VPN-Sessions an Sicherheitsprüfungen vorbei. Vor ihren bösartigen Auto-Scripts beenden die Angreifer miglogd und syslogd, außerdem löschen sie die Crash-Logs aus den Injektionsversuchen. CISA hat CVE-2025-61624 am 16.10. in den KEV-Katalog aufgenommen. Fortinet empfiehlt im Advisory zu FortiJump, Admin- und lokale Passwörter, private Schlüssel der Zertifikate, VPN-PSKs sowie RADIUS-, LDAP- und SNMP-Secrets sofort zu wechseln; für CVE-2025-61624 hilft nur FortiOS 7.6.5 bzw. 7.4.10 oder neuer, für 7.2, 7.0 und 6.4 gibt es keinen Fix. Unsere Einschätzung: Nach unserer

Erfahrung sitzt FortiGate bei vielen Stadtwerken als VPN-Gateway und Firewall vor der Leittechnik. Patchen allein beendet so einen Einbruch nicht, Betreiber mit FortiManager sollten nach den Indi

GESAMTBEWERTUNG

Hoch – vorrangig die Meldungen mit hoher Relevanz prüfen und umsetzen.

Lageübersicht

ID	Meldung	Relevanz
L-01	**Loxone (Kollerschlag, Österreich): Cyberangriff am Wochenende auf den Hersteller von Gebäudeautomation**: Laut Florian Wöss aus der Geschäftsführung kamen die Angreifer über einen Webserver von Loxone herein (ORF Oberösterreich, 19.10.). Nach Angaben von Loxone sind das interne CRM, das Bewerbermanagement und die Datenbank der Webseite betroffen. Die Systeme wurden isoliert und werden schrittweise wieder hochgefahren. Kopiert wurden laut Loxone Kontaktdaten von Partnerbetrieben (vor allem Elektroinstallateure), Support-Anfragen und Bewerberdaten, ein Teil davon veraltet. Gegenüber dem ORF sprach Wöss zusätzlich von abgeflossenen Kundendaten, ohne Art oder Umfang zu nennen; die schriftliche Stellungnahme bei heise nennt nur Partner-, Support- und Bewerberdaten. Zugangsdaten von Kundenanlagen liegen laut Hersteller nur lokal auf dem Miniserver. Miniserver, Remote Connect und Exosphere seien nicht betroffen, Zahlungsdaten und Quellcode ebenfalls nicht. Loxone hat die Behörden informiert und arbeitet mit externen Forensikern. Auf der verunstalteten Webseite bekannte sich die Gruppe „Samurai“ und behauptet, rund 200 GB kopiert zu haben (heise). Laut Auflistung der Angreifer (Screenshots im Loxforum) sollen auch Daten zu Microsoft-365-Konten und SSO-Logins dabei sein, dazu ein Register mit rund 300.000 Miniserver-Seriennummern und Projektnamen. Loxone hat diese Angaben nicht bestätigt. Zur Confluence-Auflistung erklärt Loxone, das LoxWiki sei ein Community-Projekt, Loxone setze kein Confluence ein. Zu einer Lösegeldforderung sagt Loxone nichts. Unsere Einschätzung: Die abgeflossenen Partnerdaten könnten gezieltes Phishing über Elektroinstallateure an Betreiber von Gebäuden und technischen Anlagen ermöglichen. Betreiber sollten prüfen, ob ihre Miniserver aus dem Internet erreichbar sind, vorsorglich wegen der behaupteten SSO- und Seriennummern-Daten die Passwörter wechseln und ihre Installateure vor gefälschten Loxone-Mails warnen. Quellen: https://www.heise.de/news/Loxone-Cyberangriff-auf-Gebaeudeautomatisierungsanbieter-11492872.html · https://ooe.orf.at/stories/3375871/	HOCH

ID	Meldung	Relevanz
L-02	**„PwnEscape“: Linux-Kernel-Lücke ermöglicht den Ausbruch aus virtuellen Maschinen (CVE-2026-99999)**: Laut heise (19.10.) und CSO Online (16.10.) steckt der Fehler im Netzwerkstack des Linux-Kernels. Über virtio-Metadaten zur Prüfsumme kann eine Gast-VM festlegen, wohin der Host-Kernel später schreibt, und der Kernel prüft diese Position falsch. heise nennt einen CVSS-Wert von 9,3. Der Forscher Paulos Yibelo (pwn.ai) konnte laut CSO 32 Byte Speicher des Hosts auslesen und im Labor, verkettet mit weiteren Techniken, Code auf dem Host ausführen. Laut heise brachten die Forscher im Labor auch Hypervisoren samt ihrer VMs zum Absturz. Der Fix ist laut CSO seit 14.10. im Mainline-Kernel und steckt in den Stable-Zweigen 5.10, 5.15, 6.1, 6.6, 6.12, 6.18 und 7.2. Debian liefert laut heise gepatchte Kernel aus (bookworm 6.1.190-1, trixie 6.12.113-1), bei Ubuntu und Red Hat standen die Updates noch aus. Unsere Einschätzung: Für OT zählt das überall, wo SCADA-Server, Historian oder Jump Hosts auf selbst betriebenen KVM-Hosts laufen, etwa unter Proxmox. Eine kompromittierte VM könnte dann die Segmentierung aushebeln. Patchen muss man den Host, ein Update in der VM reicht nicht. Quellen: ht tps://www.heise.de/news/PwnEscape-Kritische-Luecke-in-Linux-Kernel-erlau bt-VM-Ausbruch-11492131.html · https://www.csoonline.com/article/42364 60/linux-kernel-gets-a-fix-for-a-flaw-that-enabled-attackers-to-escape-vms. html	MITTEL
L-03	UPDATE: **Fortinet FortiManager und FortiOS: Unit 42 beschreibt Einbruch bei einem MSP und die Backdoor PEERSTITCH (CVE-2024-47575, CVE-2025-61624)**: Laut Unit 42 von Palo Alto Networks (Bericht vom 14.10.) ist die Gruppe CL-STA-0954 (auch UNC5820) ab September 2024 über FortiJump (CVE-2024-47575) in den FortiManager eines Managed Service Providers aus der Telekommunikation eingedrungen, der über 500 FortiGates verwaltet. Abgezogen wurden die Running-Configs dieser FortiGates, Topologie- und Routing-Daten, administrative, lokale und SSL-VPN-Zugangsdaten (als umkehrbar verschlüsselter Text gespeichert, einige Passwörter wurden laut Unit 42 per Brute Force geknackt) sowie Zertifikate mit privaten Schlüsseln. Die Netze der Endkunden hat Unit 42 nicht untersucht, dort ist nur der Abfluss von Konfigurationen und Zugangsdaten belegt, kein Einbruch. Über die Path-Traversal-Lücke CVE-2025-61624 (setzt eine Anmeldung voraus) schreiben die Angreifer als root Dateien und setzen die Backdoor PEERSTITCH ein. Sie hinterlässt kein dauerhaftes Binary auf der Festplatte (die Staging-Dateien lagen vorher unter /data2/template/), hängt sich per ptrace in die FortiOS-Prozesse iked und miglogd und lässt markierte VPN-Sessions an Sicherheitsprüfungen vorbei. Vor ihren bösartigen Auto-Scripts beenden die Angreifer miglogd und syslogd, außerdem löschen sie die Crash-Logs aus den Injektionsversuchen. CISA hat CVE-2025-61624 am 16.10. in den KEV-Katalog aufgenommen. Fortinet empfiehlt im Advisory zu FortiJump, Admin- und lokale Passwörter, private Schlüssel der Zertifikate, VPN-PSKs sowie RADIUS-, LDAP- und SNMP-Secrets sofort zu wechseln; für CVE-2025-61624 hilft nur FortiOS 7.6.5 bzw. 7.4.10 oder neuer, für 7.2, 7.0 und 6.4 gibt es keinen Fix. Unsere Einschätzung: Nach unserer Erfahrung sitzt FortiGate bei vielen Stadtwerken als VPN-Gateway und Firewall vor der Leittechnik. Patchen allein beendet so einen Einbruch nicht, Betreiber mit FortiManager sollten nach den Indi	HOCH

ID	Meldung	Relevanz
L-04	**The Register: Kriminelle greifen zunehmend Gebäudetechnik an**: Laut The Register vom 17.10. setzen Angreifer auf Folgen in der echten Welt, weil gestörte Gebäudetechnik den Druck zum Zahlen erhöht. Ein Beispiel ist das Health Sciences Centre in Winnipeg (Kanada): Nach einem Ransomware-Angriff im August 2026 fiel laut Betreiber Shared Health die zentrale Überwachung von Heizung, Lüftung und Klima aus, und neue Ausweise ließen sich nicht ausstellen. Ein Forscher von Armis schildert im Artikel außerdem ein nicht genanntes Finanzinstitut, bei dem sich Angreifer im Gebäudeleitsystem (BMS) versteckten und von dort ins IT-Netz zurückkehrten (Lateral Movement); der Artikel nennt dafür keine Primärquelle. Armis Labs meldet in seinem Bericht zu Gebäudeautomation für das 3. Quartal 2026, dass 91 % der untersuchten Systeme über unsichere Protokolle wie BACnet kommunizieren. Dragos zählt im 2. Quartal 2026 weltweit 1.140 Ransomware-Vorfälle bei Industrieunternehmen, 12 % mehr als im Quartal davor; die Zahl beruht auf Leak-Sites, und laut Dragos hat in keinem Fall die Ransomware selbst Steuerungssysteme erreicht. Unsere Einschätzung: Gebäudeautomation in Pumpwerken und Leitwarten gehört ins Asset-Inventar und in die Segmentierung. Quellen: https://www.theregister.com/security/2026/10/17/cybercrims-go-beyond-stealing-data-to-attack-physical-building-systems/5303677 · https://sharedhealthmb.ca/news-releases/2026-08-14-ransomware-incident-update/ · https://media.armis.com/rp-armis-labs-bas-q3-2026-en.pdf · https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2026	MITTEL
L-05	**SiteGuard Server Edition: Lücke in der Web Application Firewall wird ausgenutzt (CVE-2026-106931)**: Der japanische Hersteller EG Secure Solutions bestätigt in seinem Advisory vom 14.10., dass eine OS Command Injection in der Statistikfunktion bereits ausgenutzt wird. Die Funktion ist ab Werk aktiv, Angreifer brauchen aber schon lokalen Zugriff mit einfachen Rechten (CVSS 3.0: 7,8) und können dann Befehle als root bzw. SYSTEM ausführen. Betroffen sind Installationen auf Apache, Nginx und IIS ab Version 2.20, behoben ist die Lücke in 8.00 Update 5. Laut Hersteller gibt es Patches auch für Versionen ohne Support. Der Hersteller rät, vor dem Update unbedingt die „Diagnostic information“ herunterzuladen und aufzubewahren, weil Update oder Patch Angriffsspuren löschen können. In DACH ist das Produkt kaum verbreitet. Quellen: https://www.eg-secure.co.jp/siteguard/news/alert-202610-1 · https://jvn.jp/en/jp/JVN88474777/ · https://www.bleepingcomputer.com/news/security/hackers-exploit-siteguard-waf-flaw-to-run-commands-as-system-root/	MITTEL

Meldungen im Detail

L-01 **Loxone (Kollerschlag, Österreich): Cyberangriff am Wochenende auf den Hersteller von Gebäudeautomation: Laut Florian Wöss aus der Geschäftsführung kamen die Angreifer über einen Webserver von Loxone herein (ORF Oberösterreich, 19.10.). Nach Angaben von Loxone sind das interne CRM, das Bewerbermanagement und die Datenbank der Webseite betroffen. Die Systeme wurden isoliert und werden schrittweise wieder hochgefahren. Kopiert wurden laut Loxone Kontaktdaten von Partnerbetrieben (vor allem Elektroinstallateure), Support-Anfragen und Bewerberdaten, ein Teil davon veraltet. Gegenüber dem ORF sprach Wöss zusätzlich von abgeflossenen Kundendaten, ohne Art oder Umfang zu nennen; die schriftliche Stellungnahme bei heise nennt nur Partner-, Support- und Bewerberdaten. Zugangsdaten von Kundenanlagen liegen laut Hersteller nur lokal auf dem Miniserver. Miniserver, Remote Connect und Exosphere seien nicht betroffen, Zahlungsdaten und Quellcode ebenfalls nicht. Loxone hat die Behörden informiert und arbeitet mit externen Forensikern. Auf der verunstalteten Webseite bekannte sich die Gruppe „Samurai“ und behauptet, rund 200 GB kopiert zu haben (heise). Laut Auflistung der Angreifer (Screenshots im Loxforum) sollen auch Daten zu Microsoft-365-Konten und SSO-Logins dabei sein, dazu ein Register mit rund 300.000 Miniserver-Seriennummern und Projektnamen. Loxone hat diese Angaben nicht bestätigt. Zur Confluence-Auflistung erklärt Loxone, das LoxWiki sei ein Community-Projekt, Loxone setze kein Confluence ein. Zu einer Lösegeldforderung sagt Loxone nichts. Unsere Einschätzung: Die abgeflossenen Partnerdaten könnten gezieltes Phishing über Elektroinstallateure an Betreiber von Gebäuden und technischen Anlagen ermöglichen. Betreiber sollten prüfen, ob ihre Miniserver aus dem Internet erreichbar sind, vorsorglich wegen der behaupteten SSO- und Seriennummern-Daten die Passwörter wechseln und ihre Installateure vor gefälschten Loxone-Mails warnen. Quellen: https://www.heise.de/news/Loxone-Cyberangriff-auf-Gebaeudeautomatisierungsanbieter-11492872.html · https://ooe.orf.at/stories/3375871/**

Relevanz: HOCH

L-02 **„PwnEscape“: Linux-Kernel-Lücke ermöglicht den Ausbruch aus virtuellen Maschinen (CVE-2026-99999): Laut heise (19.10.) und CSO Online (16.10.) steckt der Fehler im Netzwerkstack des Linux-Kernels. Über virtio-Metadaten zur Prüfsumme kann eine Gast-VM festlegen, wohin der Host-Kernel später schreibt, und der Kernel prüft diese Position falsch. heise nennt einen CVSS-Wert von 9,3. Der Forscher Paulos Yibelo (pwn.ai) konnte laut CSO 32 Byte Speicher des Hosts auslesen und im Labor, verkettet mit weiteren Techniken, Code auf dem Host ausführen. Laut heise brachten die Forscher im Labor auch Hypervisoren samt ihrer VMs zum Absturz. Der Fix ist laut CSO seit 14.10. im Mainline-Kernel und steckt in den Stable-Zweigen 5.10, 5.15, 6.1, 6.6, 6.12, 6.18 und 7.2. Debian liefert laut heise gepatchte Kernel aus (bookworm 6.1.190-1, trixie 6.12.113-1), bei Ubuntu und Red Hat standen die Updates noch aus. Unsere Einschätzung: Für OT zählt das überall, wo SCADA-Server, Historian oder Jump Hosts auf selbst betriebenen KVM-Hosts laufen, etwa unter Proxmox. Eine kompromittierte VM könnte dann die Segmentierung aushebeln. Patchen muss man den Host, ein Update in der VM reicht nicht. Quellen: https://www.heise.de/news/PwnEscape-Kritische-Luecke-in-Linux-Kernel-erlaubt-VM-Ausbruch-11492131.html · https://www.csoonline.com/article/4236460/linux-kernel-gets-a-fix-for-a-flaw-that-enabled-attackers-to-escape-vms.html**

Relevanz: MITTEL

L-03 UPDATE: **Fortinet FortiManager und FortiOS: Unit 42 beschreibt Einbruch bei einem MSP und die Backdoor PEERSTITCH (CVE-2024-47575, CVE-2025-61624): Laut Unit 42 von Palo Alto Networks (Bericht vom 14.10.) ist die Gruppe CL-STA-0954 (auch UNC5820) ab September 2024 über FortiJump (CVE-2024-47575) in den FortiManager eines Managed Service Providers aus der Telekommunikation eingedrungen, der über 500 FortiGates verwaltet. Abgezogen wurden die Running-Configs dieser FortiGates, Topologie- und Routing-Daten, administrative, lokale und SSL-VPN-Zugangsdaten (als umkehrbar verschlüsselter Text gespeichert, einige Passwörter wurden laut Unit 42 per Brute Force geknackt) sowie Zertifikate mit privaten Schlüsseln. Die Netze der Endkunden hat Unit 42 nicht untersucht, dort ist nur der Abfluss von Konfigurationen und Zugangsdaten belegt, kein Einbruch. Über die Path-Traversal-Lücke CVE-2025-61624 (setzt eine Anmeldung voraus) schreiben die Angreifer als root Dateien und setzen die Backdoor PEERSTITCH ein. Sie hinterlässt kein dauerhaftes Binary auf der Festplatte (die Staging-Dateien lagen vorher unter /data2/template/), hängt sich per ptrace in die FortiOS-Prozesse iked und miglogd und lässt markierte VPN-Sessions an Sicherheitsprüfungen vorbei. Vor ihren bösartigen Auto-Scripts beenden die Angreifer miglogd und syslogd, außerdem löschen sie die Crash-Logs aus den Injektionsversuchen. CISA hat CVE-2025-61624 am 16.10. in den KEV-Katalog aufgenommen. Fortinet empfiehlt im Advisory zu FortiJump, Admin- und lokale Passwörter, private Schlüssel der Zertifikate, VPN-PSKs sowie RADIUS-, LDAP- und SNMP-Secrets sofort zu wechseln; für CVE-2025-61624 hilft nur FortiOS 7.6.5 bzw. 7.4.10 oder neuer, für 7.2, 7.0 und 6.4 gibt es keinen Fix. Unsere Einschätzung: Nach unserer Erfahrung sitzt FortiGate bei vielen Stadtwerken als VPN-Gateway und Firewall vor der Leittechnik. Patchen allein beendet so einen Einbruch nicht, Betreiber mit FortiManager sollten nach den Indi**

Relevanz: HOCH

L-04 **The Register: Kriminelle greifen zunehmend Gebäudetechnik an: Laut The Register vom 17.10. setzen Angreifer auf Folgen in der echten Welt, weil gestörte Gebäudetechnik den Druck zum Zahlen erhöht. Ein Beispiel ist das Health Sciences Centre in Winnipeg (Kanada): Nach einem Ransomware-Angriff im August 2026 fiel laut Betreiber Shared Health die zentrale Überwachung von Heizung, Lüftung und Klima aus, und neue Ausweise ließen sich nicht ausstellen. Ein Forscher von Armis schildert im Artikel außerdem ein nicht genanntes Finanzinstitut, bei dem sich Angreifer im Gebäudeleitsystem (BMS) versteckten und von dort ins IT-Netz zurückkehrten (Lateral Movement); der Artikel nennt dafür keine Primärquelle. Armis Labs meldet in seinem Bericht zu Gebäudeautomation für das 3. Quartal 2026, dass 91 % der untersuchten Systeme über unsichere Protokolle wie BACnet kommunizieren. Dragos zählt im 2. Quartal 2026 weltweit 1.140 Ransomware-Vorfälle bei Industrieunternehmen, 12 % mehr als im Quartal davor; die Zahl beruht auf Leak-Sites, und laut Dragos hat in keinem Fall die Ransomware selbst Steuerungssysteme erreicht. Unsere Einschätzung: Gebäudeautomation in Pumpwerken und Leitwarten gehört ins Asset-Inventar und in die Segmentierung. Quellen: https://www.theregister.com/security/2026/10/17/cybercrims-go-beyond-stealing-data-to-attack-physical-building-systems/5303677 · https://sharedhealthmb.ca/news-releases/2026-08-14-ransomware-incident-update/ · https://media.armis.com/rp-armis-labs-bas-q3-2026-en.pdf · https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2026**

Relevanz: MITTEL

L-05 **SiteGuard Server Edition: Lücke in der Web Application Firewall wird ausgenutzt (CVE-2026-106931): Der japanische Hersteller EG Secure Solutions bestätigt in seinem Advisory vom 14.10., dass eine OS Command Injection in der Statistikfunktion bereits ausgenutzt wird. Die Funktion ist ab Werk aktiv, Angreifer brauchen aber schon lokalen Zugriff mit einfachen Rechten (CVSS 3.0: 7,8) und können dann Befehle als root bzw. SYSTEM ausführen. Betroffen sind Installationen auf Apache, Nginx und IIS ab Version 2.20, behoben ist die Lücke in 8.00 Update 5. Laut Hersteller gibt es Patches auch für Versionen ohne Support. Der Hersteller rät, vor dem Update unbedingt die „Diagnostic information“ herunterzuladen und aufzubewahren, weil Update oder Patch Angriffsspuren löschen können. In DACH ist das Produkt kaum verbreitet. Quellen: https://www.eg-secure.co.jp/siteguard/news/alert-202610-1 · https://jvn.jp/en/jp/JVN88474777/ · https://www.bleepingcomputer.com/news/security/hackers-exploit-siteguard-waf-flaw-to-run-commands-as-system-root/**

Relevanz: MITTEL

Einordnung und Unterstützung: OT-Cyber.de · Am Esbaum 12, 83022 Rosenheim · +49 8031 8603164 · akademie@ot-cyber.de · https://ot-cyber.de/